

TOWARDS A USABLE FALLBACK AUTHENTICATION MECHANISM

A Project

Presented to the faculty of the Department of Computer Science

California State University, Sacramento

Submitted in partial satisfaction of
the requirements for the degree of

MASTER OF SCIENCE

in

Computer Science

by

Radha Dhekane

SPRING
2020

© 2020

Radha Dhekane

ALL RIGHTS RESERVED

TOWARDS A USABLE FALLBACK AUTHENTICATION MECHANISM

A Project

by

Radha Dhekane

Approved by:

_____, Committee Chair
Dr. Yuan Cheng

_____, Second Reader
Dr. Xiaoyan Sun

Date

Student: Radha Dhekane

I certify that this student has met the requirements for format contained in the University format manual, and this project is suitable for electronic submission to the library and credit is to be awarded for the project.

_____, Graduate Coordinator
Dr. Jinsong Ouyang

Date

Department of Computer Science

Abstract
of
TOWARDS A USABLE FALLBACK AUTHENTICATION MECHANISM
by
Radha Dhekane

Fallback authentication recovers user access in case a user is unable to log back in or has forgotten the password. Security questions are one of the means for fallback authentication. However, security questions are not as robust as we think and can cause a security breach by enabling unauthorized access. Along with security, usability is a growing concern for the effective use of security questions.

It is crucial to expose the vulnerability of security questions and establish a new approach to improve its usability. We conduct an online user survey to validate user opinions for the usability of text-based security questions. We then conduct another on-campus study in a span of six weeks to specifically examine the memorability aspect of security questions.

There are several known attacks against security questions, such as man-in-the-middle (MITM) attacks, brute force attacks, or keystroke logging attacks. We implement a password reset MITM simulation that exploits user accounts by either answering their

security questions or compromising the OTP (one-time-passwords) sent to the victims' phones or email addresses.

The project also proposes an alternative knowledge-based security question mechanism based on recognition rather than recall. We adopt a hybrid approach to make the validation more robust. Furthermore, we suggest how security question guidelines can be adapted to enhance its usability.

_____, Committee Chair
Dr. Yuan Cheng

Date

ACKNOWLEDGEMENTS

First and foremost, I want to express my sincere gratitude to Dr. Yuan Cheng for giving me the guidance and the confidence to pursue this project. Your vision, motivation, and dedication inspire me.

I want to thank Dr. Xiaoyan Sun, for her support and timely feedback.

I would like to thank Dr. Jinsong Ouyang, for guiding me throughout my graduate journey at CSUS.

I would like to thank my parents for believing in me and motivating me to achieve my goals.

I would also like to thank the CSUS library for providing access to databases and security articles.

TABLE OF CONTENTS

Page

Acknowledgments	vii
List of Tables	x
List of Figures.....	xi
Chapter	
1. INTRODUCTION.....	1
1.1 Overview	2
1.2 Organization	3
2. LITERATURE SURVEY	5
2.1 Current Fallback Authentication Mechanisms	5
2.2 Usability of Security Questions	6
2.3 Security of Security Questions	7
2.4 Image and Sound Based Authentication Techniques	8
3. OVERVIEW OF SECURITY QUESTIONS.....	10
3.1 Types of Security Questions.....	10
3.2 Characteristics of Security Questions	11
3.3 Issues with Security Questions	12
4. SURVEY ON USABILITY OF SECURITY QUESTIONS	14
4.1 Fallback Authentication Techniques	15
4.2 Built-in Security Questions Vs User Generated Security Questions	16

4.3	Memorability of Security Questions	17
4.4	Time Between Enrollment and Application of Security Questions.....	20
4.5	Survey Findings.....	22
5.	THREATS TO FALLBACK AUTHENTICATION MECHANISMS.....	23
5.1	Types of Attacks	23
5.2	Implementation of MITM attack	24
6.	PROPOSED THEME-BASED APPROACH.....	33
6.1	Recognition Vs Recall.....	33
6.2	Proposed Design.....	34
7.	CONCLUSION AND FUTURE WORK.....	38
7.1	Conclusion.....	38
7.2	Future Work.....	38
	Appendix A: Screening Survey	40
	Appendix B: Security Questions Survey	43
	Bibliography	48

LIST OF TABLES

Tables	Page
1. User Memorability to Built-in Security Questions.....	19
2. User Memorability to User-generated Security Questions.....	19

LIST OF FIGURES

Figures	Page
1. High-level Approach	3
2. Fallback Authentication Techniques	15
3. Built-in Vs User-generated Security Questions	17
4. Memorability of Security Questions	18
5. Time Between Enrollment and Application	20
6. In-class Experiment Results	21
7. Login Page of Attacker's Website.....	25
8. Attacker's Website Registration Page	26
9. Attacker Initiates Password Reset	26
10. Password Reset Options on Authenticated Account	27
11. PR-MITM Attack Using Security Questions	28
12. Security Questions on Attacker's Site	29
13. Security Questions on Authenticated Site	29
14. A Successful PR-MITM Attack	30
15. PR-MITM Attack Using OTP	31
16. Fake OTP Message from the Attacker's Site	32
17. Successful OTP Request.....	32
18. Associating Images with Sound	34
19. Registration Phase of Theme-based Approach.....	36
20. Recall Phase of Theme-based Approach	37

CHAPTER 1

INTRODUCTION

Nowadays, security has become one of the most pressing issues of the Internet. Passwords have been extensively used for primary authentication mechanisms [1]. Choosing a robust password is imperative for maintaining account security. Along with keeping a secure password, one must ensure that the fallback authentication is resilient to threats, since a weak password recovery mechanism will also render passwords insecure. Security questions are a popular and extensively utilized fallback authentication mechanism. A recent Google study emphasized that security questions alone are not robust enough to be used as a single fallback authentication mechanism [2]. They can be easily inferred through social engineering attacks. It is also important to analyze the usability of security questions. Memorability is a fundamental factor while considering the usability of security questions. Unlike passwords, security questions are less frequently accessed, so their recall rate is relatively low [3]. Poor usability and inadequate level of security have motivated us to seek different authentication approaches.

To address the need for a secure and usable fallback authentication mechanism, we explored the vulnerabilities of security questions. We investigated different types of attacks and threats to security questions and implemented a man-in-the-middle attack that initiated a password reset process on a victim's email account. We conclusively proposed an innovative knowledge-based fallback authentication approach that can counter the disadvantages of security questions.

1.1 Overview

Conducting user surveys helped us get feedback about the current fallback mechanisms. It also guided us to design a more robust and usable fallback authentication. We conducted two surveys. The first survey focused on getting users' views on the usability and security of security questions. The results of the first survey signified that users are not satisfied with the usability of security questions and mentioned that their security needed improvement. The second survey was a two-round survey to specifically investigate the memorability aspect of these questions. Users were asked to recall their answers to security questions after a six-week gap. The recall rate was observed to be very low, and users were not able to answer many questions accurately. Analyzing both surveys helped understand the usability concerns of security questions as well as what measures needed to be taken to improve the memorability. The surveys were vital in guiding us to find an alternative approach.

Security questions can be breached by man-in-the-middle attacks, brute force attacks, or keystroke logging attacks. We implemented a known password reset man-in-the-middle attack (PR-MITM) attack [4]. The purpose of this MITM attack was to expose that if the password reset mechanisms are weak, a user's account can get compromised. The MITM attack was able to compromise the victim's security questions and proceed with the password reset on the victim's mail account.

Since security questions are based on the recall aspect of memorability, we propose a theme-based approach, based on recognition, which is faster and easier to perform. The proposed idea also includes adapting the theory of intrinsic memorability for visuals and

sounds. The new approach combines the use of graphical information and non-speech sound to invoke associative memory potential. This approach provides user a choice to select and design their own theme, which makes it simpler and more user-friendly approach. Figure 1 shows the high-level approach of this project.

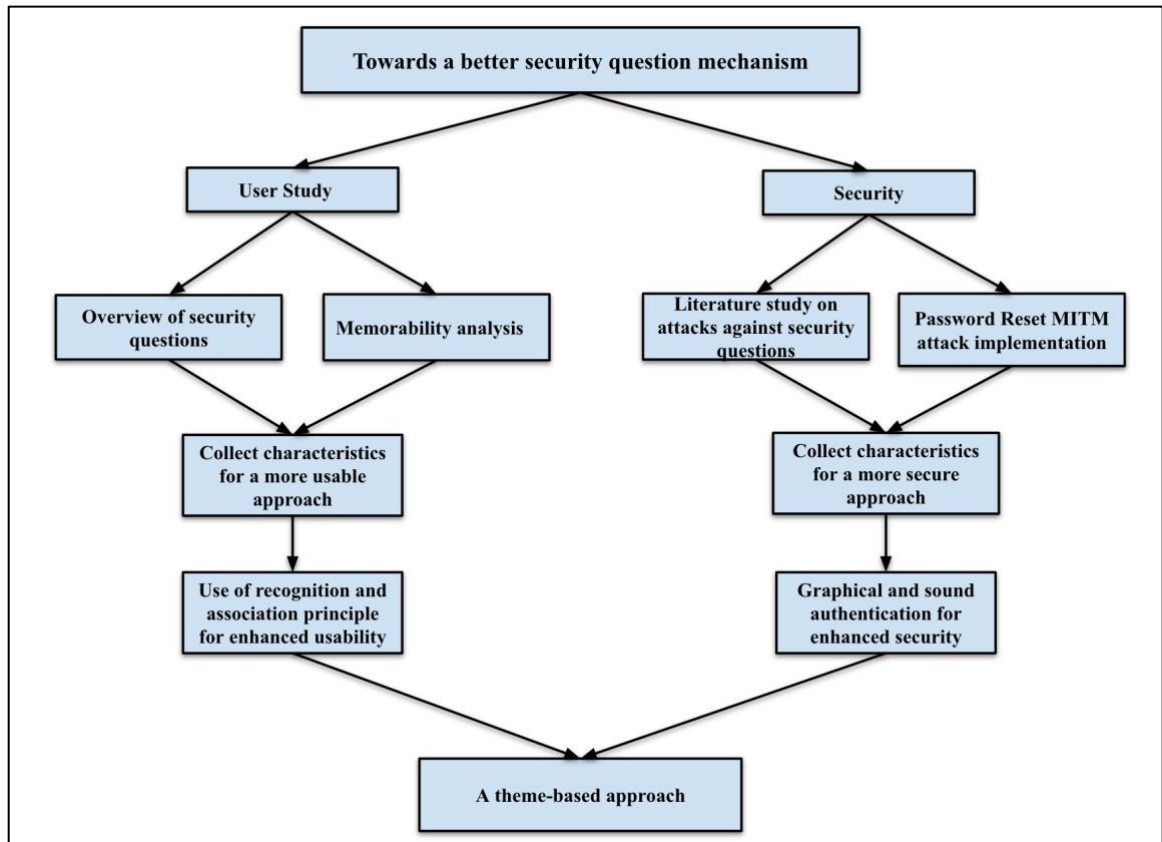


Figure 1: High-level Approach

1.2 Organization

The remainder of the report is organized as follows. In Chapter 2, we survey the previous research work and lay a conceptual foundation for the study. We analyze the characteristics and shortcomings of security questions in Chapter 3. We present a user

study that highlights user opinions and user perception on security questions in Chapter 4. We then investigate the types of threats to security questions and implement a password reset man-in-the-middle attack in Chapter 5. In Chapter 6, we propose a novel knowledge-based approach that uses visual and audio associations to improve the usability of fallback authentication. In Chapter 7, we provide a conclusion and a direction for future work.

CHAPTER 2

LITERATURE SURVEY

2.1 Current Fallback Authentication Mechanisms

There are several widely deployed fallback authentication mechanisms, ranging from inherence-based authentication systems (biometrics), knowledge-based authentication systems (e.g., security questions and passwords) to possession-based authentication systems (e.g., tokens, security cards, etc.) [5]. Multi-factor authentication techniques such as SMS and email verification are currently popular fallback mechanisms. Password reset emails are not encrypted, they can be breached by man-in-the-middle (MITM) attacks. Email verification can also cause a single point of failure if the email account has been compromised [6]. These schemes are also unable to work in case of failure to access the email or if the phone number does not exist [7]. Moreover, people with low usage of smartphones (e.g., senior citizens) may not prefer such fallback mechanisms.

In the SMS verification, a user gets a one-time password (OTP) on her registered phone. Once she submits the OTP, she is redirected to reset the account password. SMS authentication has several drawbacks. Each message sent has a cost associated with it. Also, OTP messages can be intercepted by password reset man-in-the-middle attacks [4]. If there is no cellular network or in case of phone damage, SMS verification would fail to let the user log in to her account.

Another popular fallback authentication mechanism is social authentication. If a user is unable to log in to her account, a few of her close contacts can send him a link to

log back in. Javed et al. presented the Trusted Friend Attack, which was able to compromise Facebook's social authentication mechanism by exploiting client-side tests [3]. The drawback of social authentication is that recovering an account can take much time varying from several hours to days, depending on the availability of the trusted contacts.

2.2 Usability of Security Questions

Earlier studies by Zviran et al. on the usability of cognitive techniques claimed that security questions had superior recall rates over other traditional approaches, such as passphrases [8]. In a recent Google study, Bonneau et al. analyzed loopholes in the usability of security questions through statistical analysis of different parameters [2]. They assessed that the most secure questions have the lowest recall rates. Google stopped the use of security questions in 2019 after examining its unreliability and poor security standard for account recovery [2].

Just et al. inspected the usability of user-generated questions and answers [9]. Based on the designed model, the authors claimed that user-chosen questions and answers suffer from low entropy issues, in which the answer space of security questions is limited. A self-assessment study was also conducted to check the memorability of the answers. The outcome of the study signified a need for a novel and usable approach.

Different alternatives have been recommended to enhance the usability of security questions. Hang et al. proposed a theory on location-based personal knowledge questions [10]. It uses a map-based input to identify a user's location. Users will highlight their locations on the map based on the question and will update them on the world map

accordingly [10]. The user study was conducted on a small population of 30 candidates. Although the author's claim that the newly proposed design is more secure and usable than text-based questions, it can still fall prey to social engineering attacks by close adversaries. Also, answering map-based questions may be more time-consuming than answering text-based security questions.

2.3 Security of Security Questions

A recent Google study on security questions claims that security offered by these questions is far lower than primary authentication mechanisms such as passwords [2]. There is a risk of statistical attacks since many users provide similar answers to common security questions. Senarath et al. proposed a user design mechanism to improve the strength of security question answers [11]. The design involved providing visual feedback to the users indicating the strength of their security answers. The metric to measure strength was based on the length of the answer. Although an innovative approach to nudge users to provide more robust answers, security questions are based on cued recall, and the type of question can profoundly influence the answer space.

Another potential approach suggested by Micallef et al. is the use of 'avatars,' which encourages a user to answer system-generated questions based on an 'avatar,' i.e., a fictitious character [12]. It prepares a set of security questions based on that character's profile created at registration. It would be difficult to ascertain the information about the avatar and thus would help to mitigate social engineering attacks. This scheme, however,

adds time overhead. Answering questions based on the profile of a character would also cause memorability issues for users in the long run.

2.4 Image and Sound Based Authentication Techniques

Studies confirm that images are easier to recall than text-based input [13]. We analyze a few graphical schemes that display enhanced usability than other authentication techniques.

Akula et al. proposed an image-based authentication scheme named IBRAS (Image-Based Registration and Authentication System) [14]. Upon registration, users provide their user IDs and get a set of images from which they select an image of their choices as a password. As humans are good at recognizing visual data, it helps to remember their password vividly. The system is more secure, as the hashed value of the image, rather than the image itself, is store in the database.

Almuairfi et al. presented an Implicit Password Authentication System (IPAS), which is more secure and invulnerable to common attacks like screen-dump attack and shoulder-surfing attack [15]. While logging to the system, a user has to select the grid-of-interest correctly to get authenticated by the system. IPAS requires human interaction and user training for selecting the appropriate points of the image.

Ramsey et al. presented a sound-based authentication scheme where they proposed to collect features of everyday sounds that drive user's memorability using an auditory memory game [16]. The findings concluded that familiar and clear sounds have higher recall rates and can serve as triggers to memory.

The use of images in passwords has been widely researched, since image-based authentication techniques offer a good trade-off between memorability and security [17]. Their application in fallback authentication schemes needs to be explored. However, too much of graphical data can cause information overload. We offer to propose a novel solution for fallback authentication that establishes a balance of usability and security.

CHAPTER 3

OVERVIEW OF SECURITY QUESTIONS

Recovering the passwords is a challenging process, where the websites need to confirm that a user can substantiate her identity without providing primary authentication information. Security questions (also known as personal knowledge questions or challenge questions) is a concept that is extensively used in user authentication [18]. When a user tries to recover her password, in most cases, she encounters a security question, like “what’s your mother’s maiden name?”. If the user’s response is correct, she obtains the password or an option to reset the password.

3.1 Types of Security Questions

Security questions are primarily classified into two types: sensitive security questions and personal security questions [3]. Security questions that ask about sensitive information such as social security number, bank account number, and ATM codes are classified as sensitive security questions. Such types of security questions are usually asked by financial institutions that maintain details of the user’s confidential information. Personal history, family background, such as mother’s maiden name, etc., are part of personal security questions. Such types of questions are more prevalent than sensitive security questions and are more vulnerable to social engineering attacks.

Upon registration of an account, a user is asked to provide information such as user id, email address, telephone number, etc. To secure the account, he is presented with a couple

of security questions. Generally, users are given an option to pick out any two security questions of their choice out of the given system-generated questions. The answers provided at the time of registration confirm that the users are the legitimate account holders. In case a user forgets her password, he can initiate a password recovery process by answering the security questions. If the given answer matches the recorded answer, then the user can access her account and proceed with the password reset. Ideally, the answers to the security question should be known only to the user and should be easy to remember. Correct answers to such questions provide authentication proof that a genuine user is trying to access the account.

3.2 Characteristics of Security Questions

Many popular websites use security questions as a fallback authentication approach. Gary Scottville provided a study on characteristics of security questions [19]. He stated that a good security question should meet the following measures:

1. Memorable - A good security question should be easy to remember. Since Fallback authentication methods are used less frequently than passwords, they should be easy to memorize.
2. Consistent - The answers to security questions should not change over a period of time.
3. Safe - A good security question should have many plausible answers. Security questions with limited answer choices can make it easy for the attacker to brute force it.

4. Simple - It should have a precise and fixed format.
5. Secure - Security Questions should have high entropy.

Security questions are part of knowledge-based authenticated systems [5]. It is the simplest form of fallback authentication. There are a few advantages to security questions. It does not have any hardware costs associated with it. Unlike passwords, which are considered as a free recall task, the use of security questions helps in a cued recall. There is a question provided which acts as a cue that aids in memory retrieval.

3.3 Issues with Security Questions

Security questions suffer from fundamental flaws. People share overwhelming personal information on social media forums, making it easier for hackers to obtain information and answers to security questions. The answers to security questions also might change over time, and that might create a hassle for legitimate users to log back in. Security questions also suffer from applicability issues. Questions about a user's first pet or marriage anniversaries won't apply to all.

Current security questions generally ask for personal information in text-based format like:

1. Which city did you meet your spouse?
2. What is the name of your elementary school?
3. What is your mother's maiden name?

We do not realize how much of our personal information we unintentionally leak on social media. Security questions also suffer from low entropy issues. Questions such as 'What is your favorite color?' or 'What is your favorite basketball team?' have a limited

answer space. Such questions are easy to guess using a few tries and can be easily tackled by attackers. Bonneau et al. conveyed that the reliability of secret questions is not adequate [2]. They stated that the cultural background of users strongly biases the answer to secret questions (e.g., favorite foods, birthplace etc.). Statistical brute force attacks against secret questions are also a threat because many users provide similar answers to common security questions. Also, if there is no rate-limiting to guess these answers, it increases the chances of hacking a user account.

CHAPTER 4

SURVEY ON USABILITY OF SECURITY QUESTIONS

To ascertain the usability of security questions, we performed an online survey to check the vulnerability and usability of security questions. The study was undertaken by more than 150 candidates. All the candidates were above 18 years of age. The Human Intelligence Task (HIT) rate of the candidates was 90+. Most of the candidates were from the US and India and a few from Europe. The survey was hosted on Qualtrics which is an online research and survey tool. Workers were invited to take part and given incentives through Amazon Mechanical Turks. The aim of the survey with public response was to get the user's familiarity with security questions. The survey was anonymous. With the help of the survey response, we got the users' perspective on the usability and security of security questions. The user study is approved by the institutional review board (IRB). We have used Qualtrics and Tableau as the tools for data visualization. We asked the candidates in the screening survey whether they have answered security questions earlier before. 87.58% of the survey population responded that they have answered security questions for password reset. The rest of the survey was advanced for the users who were familiar with the concept of security questions and have answered security questions at least once for account recovery. About 76.03% of the survey population who answered the question agreed to the statement that there is a plausibility that someone might hack the primary email account by using security questions. This indicates that according to the user's opinion, security questions alone are not robust enough and can easily fall prey to social

engineering attacks. People reveal a ton of information on their social media platforms which makes it easy to guess answers to their security questions.

4.1 Fallback Authentication Techniques

Currently deployed fallback authentication techniques, such as security questions, email resets, and OTP authentication, suffer from usability and security concerns. We asked the survey users about what fallback authentication method do they prefer and the reasons for it.

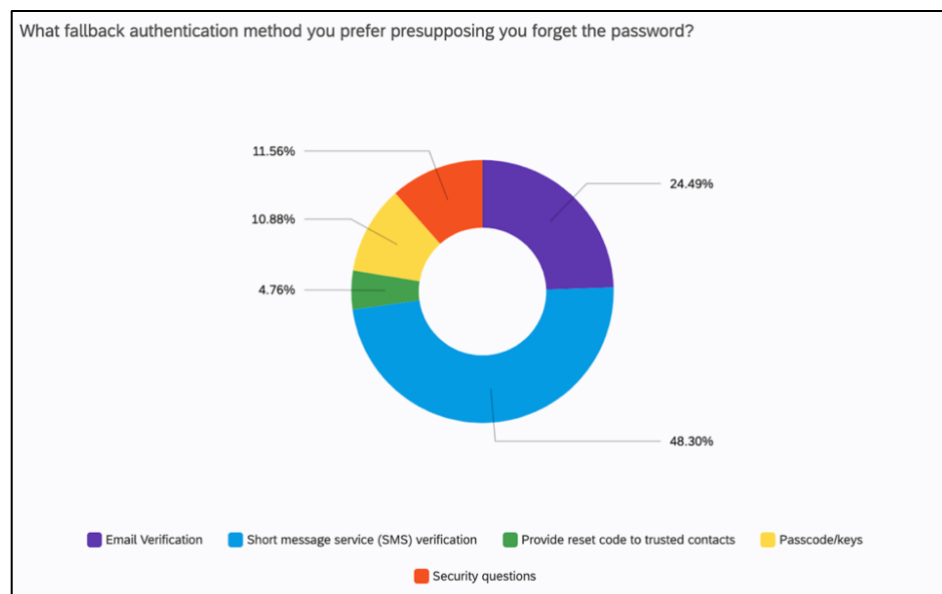


Figure 2: Fallback Authentication Techniques

As seen in Figure 2, about 48.30% of the survey population chose SMS verification as their preferred method of fallback authentication, 24.49% chose email verification and a mere 11.56% chose security questions. 10.88% chose passcode/keys and 4.76% chose to

provide code to trusted contacts. The survey population that chose SMS verification stated that it is easy, fast, convenient and that it would be difficult for potential criminals to get access to it. A few of them mentioned that since they find it difficult to remember the answers to their security questions, they prefer SMS verification. A survey respondent stated that since OTP would be valid for a short duration of time, it would be difficult to get access to it. The survey population who preferred email verification stated that it is the quickest and safest method with no extra data charges. Users who did not possess a phone or did not want to disclose their number opted for email verification. Users who chose security questions stated that they perceived security questions to be easy, safe and tailored to the individual.

4.2 Built-in Security Questions Vs User Generated Security Questions

Figure 3 displays the survey results for Built-in Vs User-generated security questions. 56.46 % of the survey population stated that they prefer user-generated security questions, i.e., provide their own questions and answers to security questions. This makes the questions more unique and specific to the user. Creating your own set of questions will avoid the issue of having generic questions and also one can have the freedom to add variations in the answers to make them difficult to guess. However, a study by Just et al. stated that user-generated security questions suffer from recall issues [9]. They are more time-consuming. Without additional assistance, there are high chances that the user might present questions that are less secure. Also, user-generated security questions suffer from low entropy, which can highly reduce the answer space, making the answer easy to guess.

We studied the memorability of built in security questions vs user generated questions in the in-class memorability experiment.

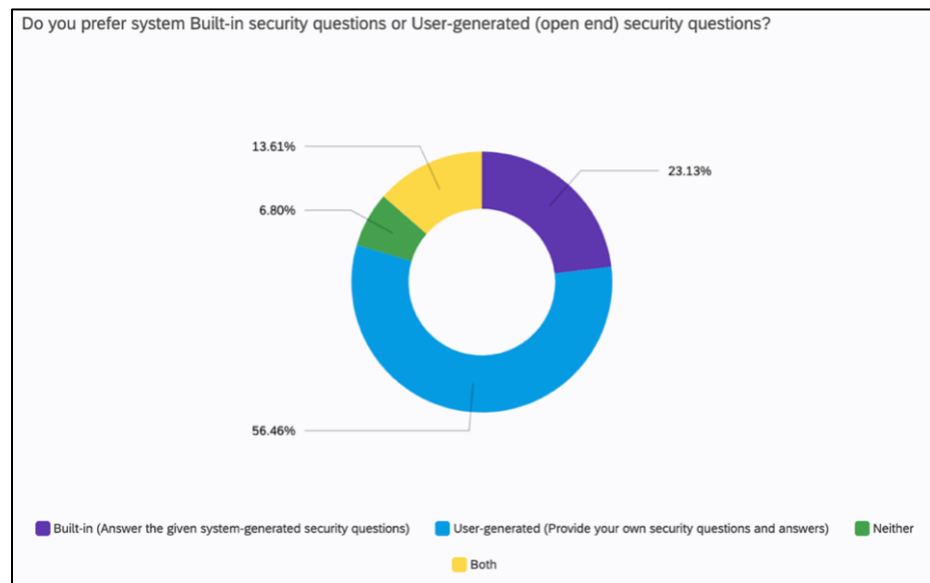


Figure 3: Built-in Vs User-generated Security Questions

4.3 Memorability of Security Questions

The first survey provided user's opinions on security questions. However, a majority of the people claimed that they remember the answers to their security questions. According to Figure 4, more than 45% of the survey population stated that they definitely remember the answers to their security questions. 44.22% claimed that they probably remember the answers to their security questions.

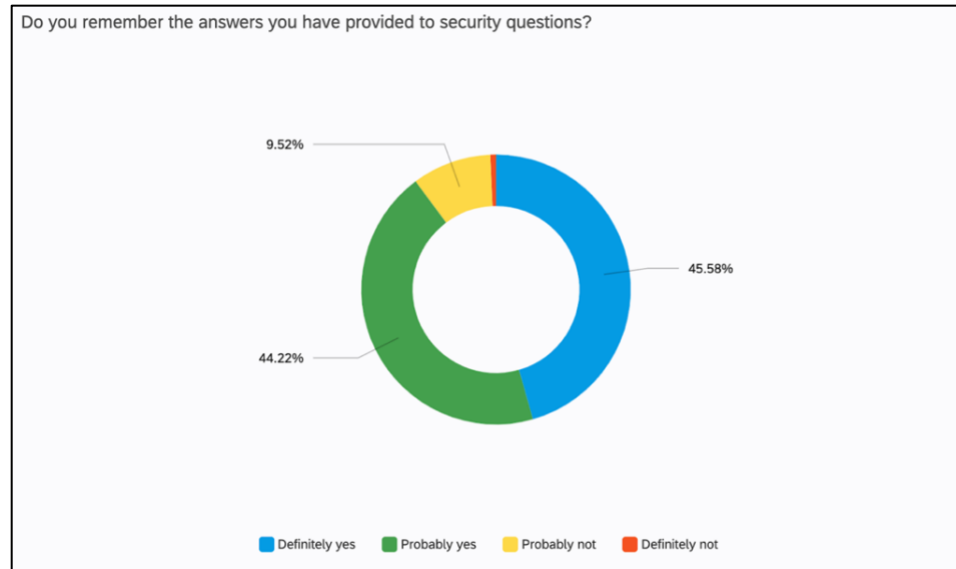


Figure 4: Memorability of Security Questions

To test this claim, we organized an in-class experiment for the memorability of security questions. The survey was taken by 48 students having computer security knowledge and background. The two-round experiment was conducted keeping a gap of six weeks. To keep the identity of students anonymous we asked them the last four digits of their student id so that we could relate the answers in the two parts of the survey.

The in-class survey contained a set of five predefined and two user-generated questions. In the memorability experiment that we conducted, students found it difficult to recall their answers to user-generated questions. We had asked users two user-generated open-end questions. In the first part of the survey, we asked the user to come up with their own question and answer. In the second part, we asked them to recall their answer to the question. The purpose of this question was primarily to check whether the user can recall their answer after six weeks without providing the cue i.e., the question. We also asked

users to choose a phrase having more than two words. The purpose of adding such questions was to test the memorability of user-generated questions.

Table 1: User Memorability to Built-in Security Questions

Built in Security Questions	Correct Answer (Match)	Incorrect Answer (Mismatch)	Couldn't Recall
Q1. Name of first pet	21	10	5
Q2. Favorite movie/book	14	4	18
Q3. Name of the street growing up	20	9	7
Q4. Last 4 digits of first phone	20	8	8
Q5. Name of first-grade teacher	11	7	18

Table 2: User Memorability to User-generated Security Questions

User generated Questions	Correct Answer (Match)	Incorrect Answer (Mismatch)	Couldn't Recall
No cue provided	6	3	27
Choose your own phrase	6	5	25

From the memorability experiment that we conducted we found that majority of the students could not recall their answers to security questions. 82.98% of the survey population claimed that they found it challenging to recall the answers to security questions. Table 1 shows the recall results to built-in security questions. 52.23% of the answers received to built-in security questions were either incorrect or students could not recall the answers to them. We also observed that majority of the user defined questions provided by the students, were either similar to built-in questions or were similar to questions having low guessing entropy such as favorite color and floor number of the apartment.

Table 2 displays the recall results to user-generated security questions. Although in the earlier survey candidates preferred user-generated questions, the recall rate for user-generated questions was a low of 16.66%. Comparing both types of questions and considering the poor result for user-generated data, we opted to provide system-generated themes in our proposed approach.

4.4 Time Between Enrollment and Application of Security Questions

One of the metrics we considered for the usability of security questions was the time duration between the enrollment phase of security questions and the application phase of security questions. As seen in Figure 5, 42.57% of users use security questions to recover their accounts, more than a year after setting them.

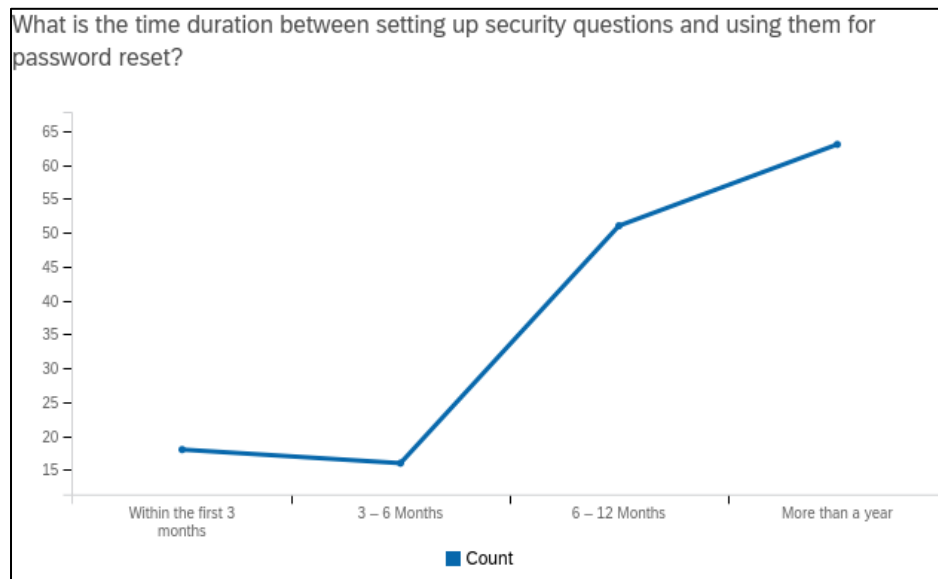


Figure 5: Time Between Enrollment and Application

The distribution is almost linear that conveys that users are likely to recover their account in the later phase of setting them. We also observed similar linear distribution in the in-class experiment as displayed in Figure 6.

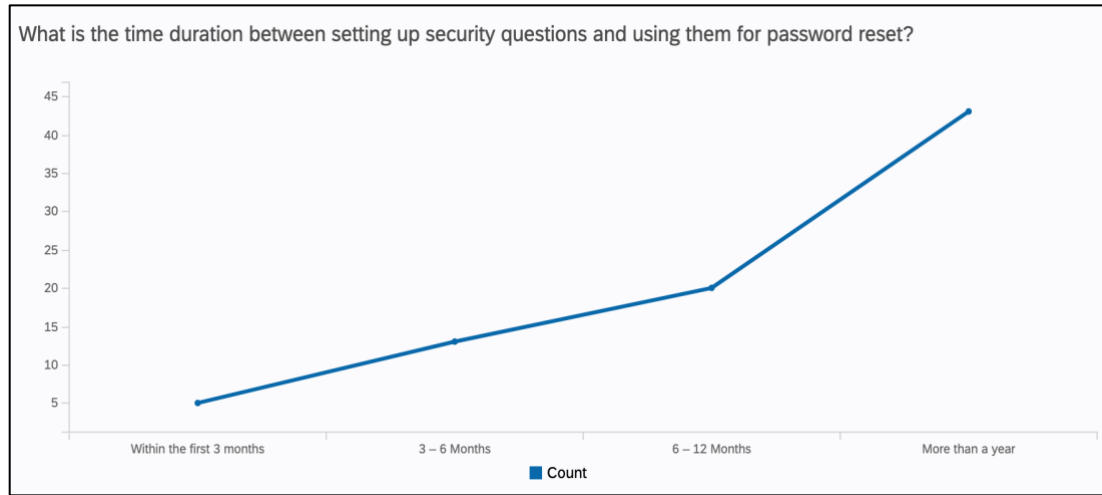


Figure 6: In-class Experiment Results

Security questions are based on recall process. The accuracy of recall depends on the study time, length of the list and delay time between the study and the test phase [20]. Figure 5 and Figure 6 show that delay time factor between the enrollment and the application is linear and gradually increasing. This decay of memorability over time possess serious usability concerns. Hence effective alternatives are needed to eradicate such memorability issues. We promote the use of recognition instead of recall to improve the memorability of answers.

4.5 Survey Findings

From analyzing the survey of 153 people, we conclude that though security questions are a simple form of fallback authentication, users currently do not prefer this mechanism since it has security and usability issues. About 63% of the population stated that they provide simple and easy answers to security questions. Although providing simple answers helps to aid in memory, it can fall prey to social engineering attacks.

Only 11.72 % preferred the use of security questions as a fallback mechanism. As the duration increases of using security questions for a password reset, users find it difficult to recall the answers. Also, about 70.62% stated in the survey that the answers to their security questions may change over a period of time which can cause uncertainty issues. Due to poor memorability, and security concerns expressed by the survey population, we can conclude that security questions if used alone, are an inferior authentication mechanism. Seeing the poor memorability result, we opted for recognition and association schemes in our proposed approach.

CHAPTER 5

THREATS TO FALLBACK AUTHENTICATION MECHANISMS

5.1 Types of Attacks

Weak authentication techniques can fall prey to attacks such as brute force attacks, keylogging attacks, and password reset man-in-the-middle attacks [4]. We investigate potential attacks that can be used against security questions and implement a password reset man-in-the-middle attack to expose the vulnerabilities of weak fallback authentication mechanism.

5.1.1 Keystroke Logging Attacks

One way to intercept the answers to security questions is through keystroke logging attacks. The attack captures the keyboard movement of a user to misuse her confidential information. Using a key logger, an attacker can get access to user data without disrupting the server operations. As the user enters her answers to security questions, the key logger stores the data in a log file [21]. The attacker can later retrieve the file from the compromised machine and obtain the data. The attacker can then use the answers to initiate a password reset process on the user's account.

5.1.2 Brute Force Attacks

Security questions suffer from low entropy; hence they can be the target of brute force attacks. In such attacks we are analyzing the guessing metrics and not exploiting any

vulnerabilities of the web application. Many websites do not keep a rate limiting cut-off to security questions which can favor such attacks. Cued recall aids in narrowing down the answer space, hence security questions are more susceptible to such attacks than passwords. According to Google reports, there is a 19.7% success rate to guess an English-speaking person's answer to what their favorite food is [2]. Brute force attacks to security questions can be abridged by the use of captchas and strict rate limiting policies.

5.1.3 Man-in-the-middle Attacks

Man-in-the-middle attack (MITM) is a type of cyber-attack in which an attacker becomes a part of a conversation between two victims. The malicious attacker compromises the communication chain between the two parties. It can lead to stealing credentials, transfer of other data, direct access to sensitive information, or can inject false information in the flow of traffic between client and server. It can intercept and steal any data submitted to the site. Such attacks can acquire user login credentials and sensitive financial information. Response time is a vital factor to be considered in such attacks.

5.2 Implementation of MITM Attack

We implemented a prototype of the password reset man-in-the-middle attack in Java. We expose how password recovery processes are vulnerable to information leaks. PR-MITM is an application-level attack. The attack can be initiated when a password reset is done by OTP on either email or phone or with the use of security questions. The MITM attack launches a password reset attack on the victim's authenticated mail account. The

attacker behaves as the man in the middle between the victim and the authenticated email service provider. The victim is lured onto the attacker's site on the pretext of downloading free software. Figure 7 shows the login page of the attacker's fake website.

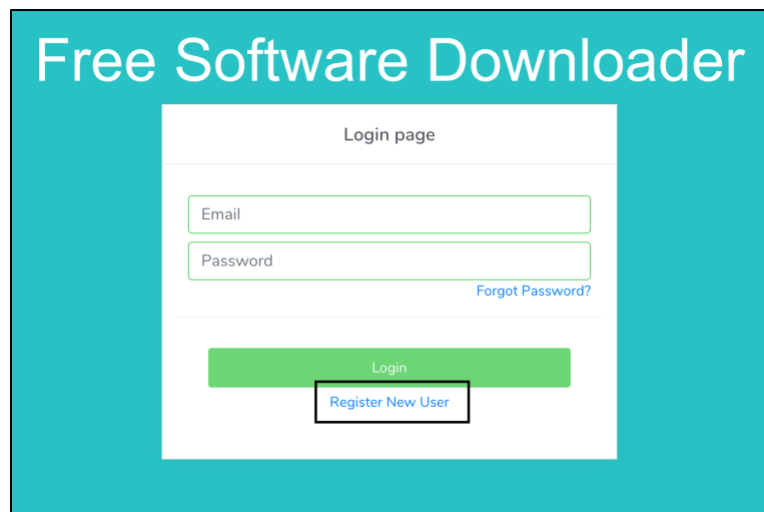
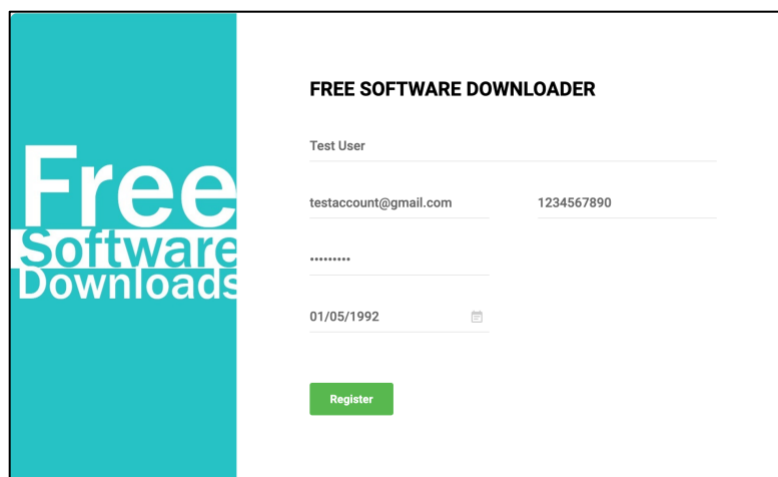


Figure 7: Login Page of Attacker's Website

As shown in Figure 8, the victim is asked to provide registration details such as email address, contact information, date of birth, etc. As soon as the attacker gets the victim's email address, he progresses towards the victim's email service provider and initiates a password reset on the authenticated email service (Figure 9).



FREE SOFTWARE DOWNLOADER

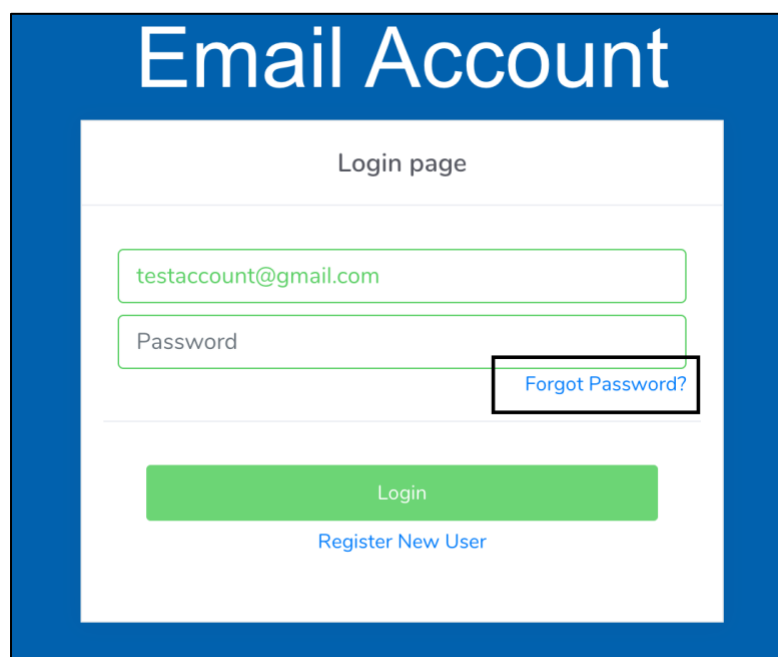
Test User

testaccount@gmail.com 1234567890

01/05/1992

Register

Figure 8: Attacker's Website Registration Page



Email Account

Login page

testaccount@gmail.com

Password

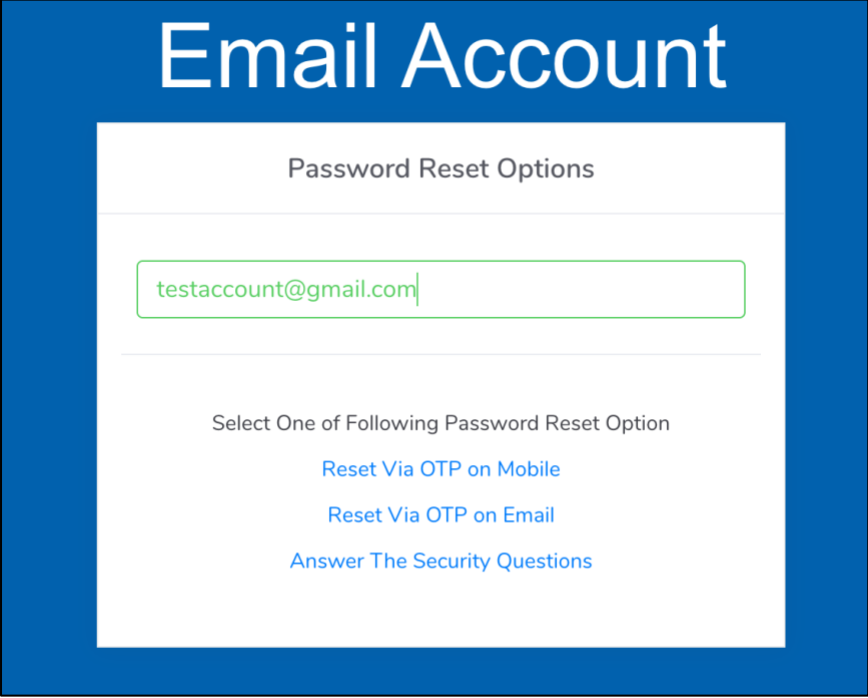
[Forgot Password?](#)

Login

[Register New User](#)

Figure 9: Attacker Initiates Password Reset

The authenticated mail service provides three options for password reset as shown in Figure 10. The password can be reset by either answering their security questions or compromising the OTP sent to the victims' phone or email addresses.



Email Account

Password Reset Options

testaccount@gmail.com

Select One of Following Password Reset Option

- [Reset Via OTP on Mobile](#)
- [Reset Via OTP on Email](#)
- [Answer The Security Questions](#)

Figure 10: Password Reset Options on Authenticated Account

5.2.1 Use of Security Questions to Reset Password

Security questions add a layer of security to protect the account from unauthorized access. When the user forgets the password, she can use security questions: a knowledge-based authentication method to reset the password. Most of the websites use a predefined standard set of security questions. Based on the survey we conducted, 91% of the user population claimed that they give truthful answers to their security questions. One part of the attack focuses on the correct answers to security questions provided by the user. Therefore, 91% of the survey population is susceptible to this password reset MITM attack. Figure 11 shows the high-level diagram of the password reset man in the middle attack using security questions.

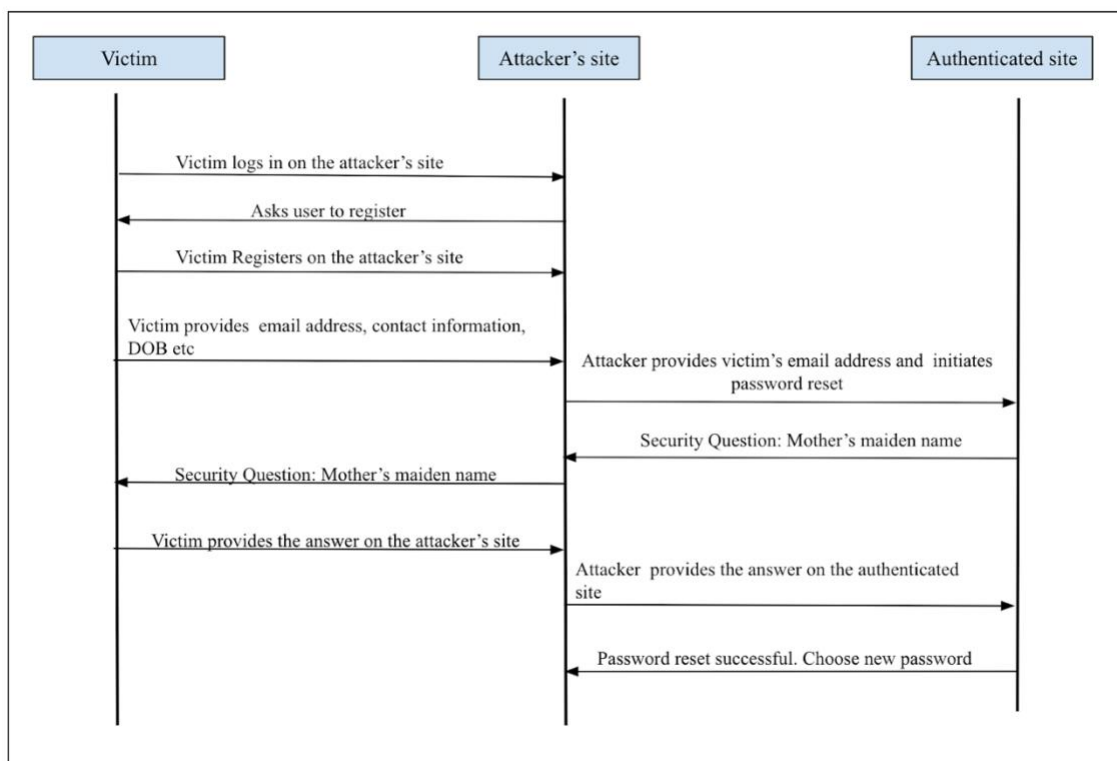
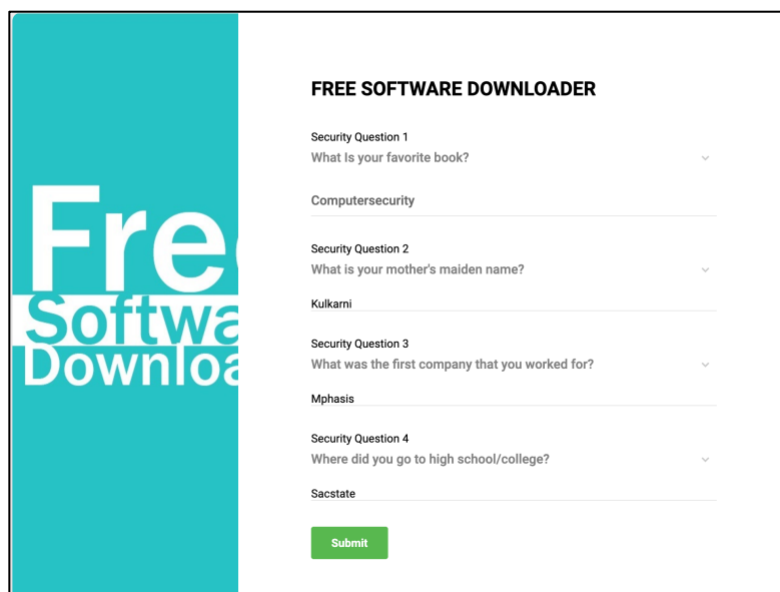


Figure 11: PR-MITM Attack Using Security Questions

Once the user registers on the attacker's site, she is asked to provide answers to four security questions as part of the registration process as displayed in Figure 12. As soon as the user provides the answer to security questions on the attacker's site, the answers along with the questions get stored in the database. These answers are then provided by the attacker on the authenticated account to initiate a password reset. Figure 13 shows security questions asked on authenticated mail service for password reset. An answer match would allow the attacker to change the password for the victim's account. Figure 14 shows a successful password reset using MITM attack.

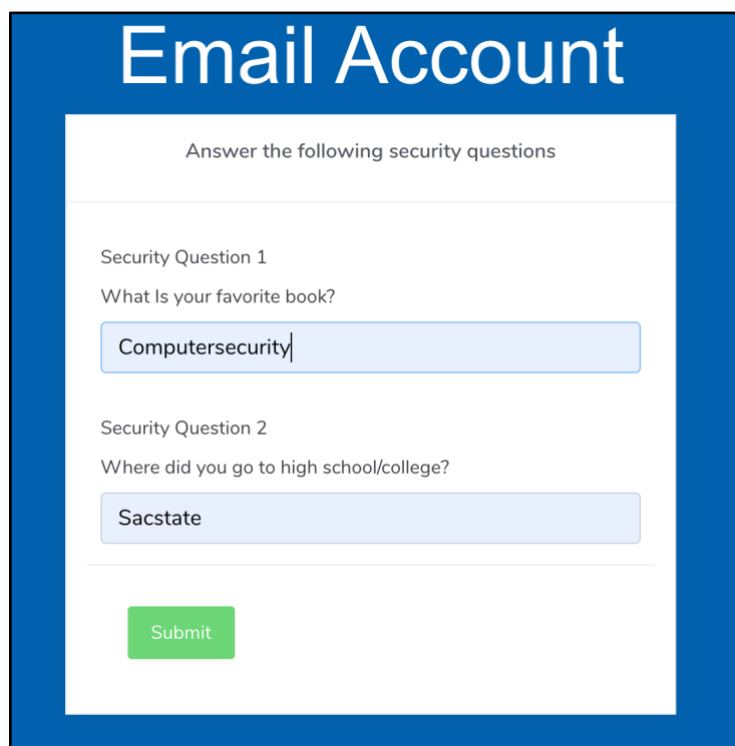


The screenshot shows a web page titled "FREE SOFTWARE DOWNLOADER". On the left, there is a teal vertical banner with the text "Free Software Download" in white. The main content area is white and contains four security questions, each with a dropdown menu and a text input field. The questions are:

- Security Question 1: What Is your favorite book? (Dropdown: Computersecurity)
- Security Question 2: What is your mother's maiden name? (Dropdown: Kulkarni)
- Security Question 3: What was the first company that you worked for? (Dropdown: Mphasis)
- Security Question 4: Where did you go to high school/college? (Dropdown: Sacstate)

At the bottom of the form is a green "Submit" button.

Figure 12: Security Questions on Attacker's Site



The screenshot shows a web page titled "Email Account" with a blue header. Below the header, there is a white box with the text "Answer the following security questions". The form contains two security questions, each with a text input field. The questions are:

- Security Question 1: What Is your favorite book? (Input: Computersecurity)
- Security Question 2: Where did you go to high school/college? (Input: Sacstate)

At the bottom of the form is a green "Submit" button.

Figure 13: Security Questions on Authenticated Site

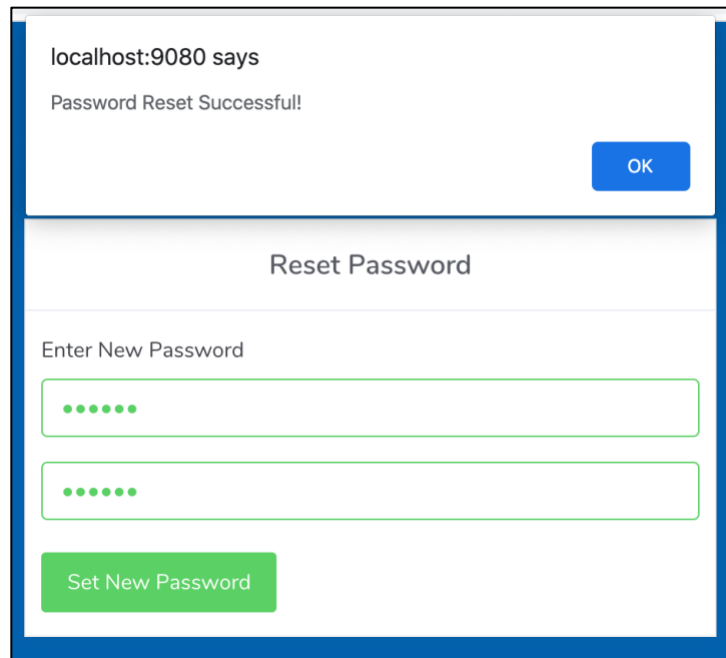


Figure 14: A Successful PR-MITM Attack

5.2.2 Use of OTP to Reset Password

An OTP is a one-time generated password valid for a short duration of time. OTP is a standard authentication method adopted by popular websites. The use of a one-time password gives advanced features like mobility, but it can be a failure if the user does not have access to the device that generates OTPs. The user has access to the device that generates an OTP using an algorithm and cryptographic keys. The authentication server can validate the OTP by matching the same algorithm and keys [22]. OTP generally ranges from four to eight digits. Figure 15 shows the high-level diagram of the password reset man-in-the-middle attack using OTP.

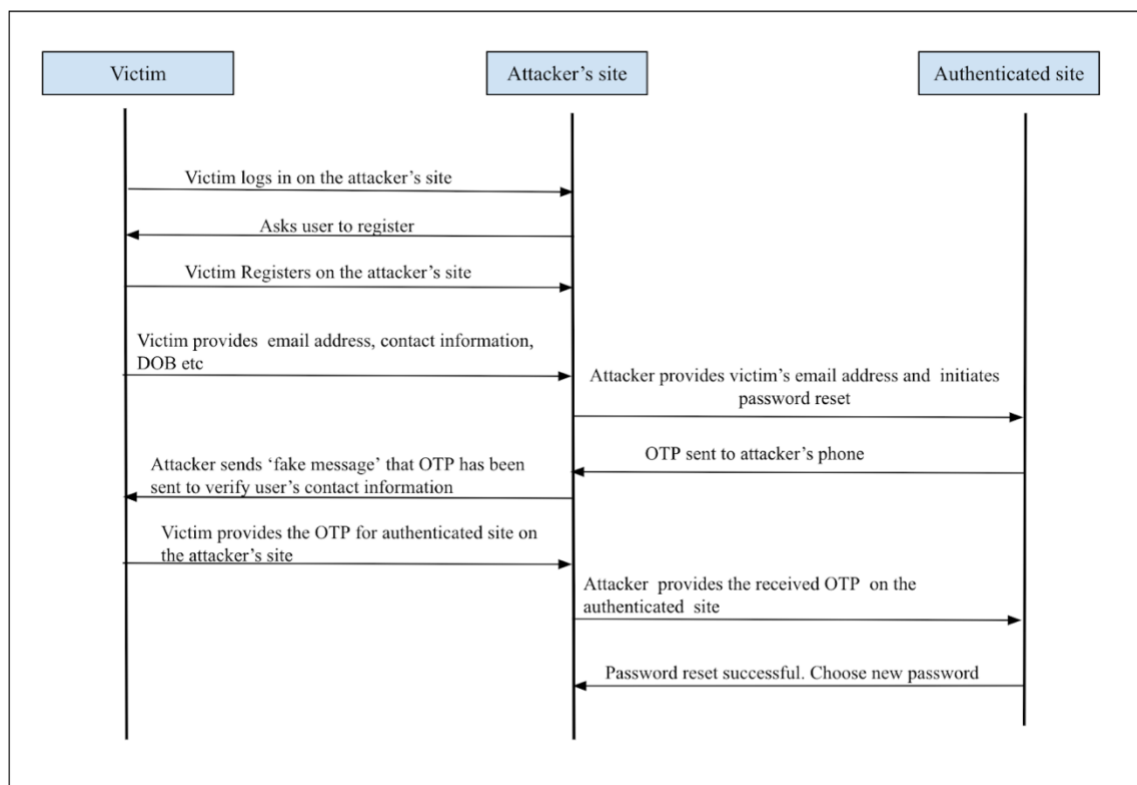
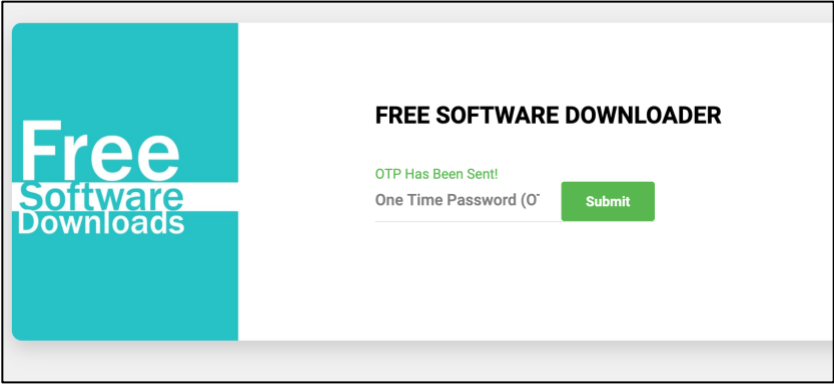


Figure 15: PR-MITM Attack Using OTP

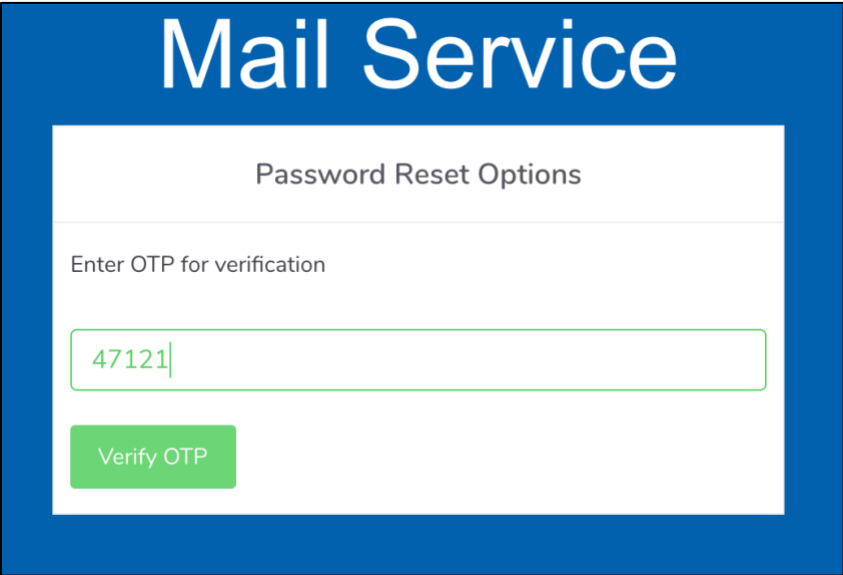
In the MITM attack, when the victim provides email and contact information, the attacker's site sends a message to the victim to check their email or phone for the OTP. Figure 16 shows the bogus OTP message from the attacker's site. Concurrently the attacker initiates the password reset process on the user's authenticated email service. The authenticated website will send an OTP to the user for proceeding with the password reset request. The message limit is generally 160 ASCII characters which is not sufficient enough to clearly provide optimal information for a password reset. It needs to include vital information such as the website information, the code for password reset, and a default warning stating not to disclose this information to others [4]. All this information is difficult to fit in the 160-character limit. Due to these limitations and less clarity observed while

sending such messages, the user may misinterpret the OTP thinking it has come from the 'fake website' and might provide the one-time password on the attacker's site. Once the attacker gets the OTP, he inputs it on the user's email service provider as shown in Figure 17 and complete the password reset process.



The screenshot shows a web page with a teal header on the left that says "Free Software Downloads". The main content area is white and titled "FREE SOFTWARE DOWNLOADER". Below the title, there is a green message that says "OTP Has Been Sent!". Underneath this message is a label "One Time Password (O" followed by a green button labeled "Submit".

Figure 16: Fake OTP Message from the Attacker's Site



The screenshot shows a blue header with the text "Mail Service". Below the header is a white box titled "Password Reset Options". Inside this box, there is a prompt "Enter OTP for verification". Below the prompt is a text input field containing the number "47121|". Below the input field is a green button labeled "Verify OTP".

Figure 17: Successful OTP Request

CHAPTER 6

PROPOSED THEME-BASED APPROACH

6.1 Recognition Vs Recall

Recognition is considered to be simpler than recall. A recall process is used to retrieve the right answer from memory, whereas recognition identifies that the provided information is correct or not [23]. Recall and recognition differ in the number of cues. It is easier to retrieve concepts from memory if we acquire a greater number of cues. These cues help to provide access to related information stored in the memory. The difference between recognition and recall is the number of cues provided by the context that aid in memory retrieval [23]. Recognition provides more number of cues than a recall process. Recall is considered to be a two-phase process. In the first phase, a possible word list is formed by looking in long-term memory. In the second phase, the words are evaluated to determine if the answer exists in the list. Recognition does not utilize the first phase. It just evaluates the given data and states whether the given information is correct or incorrect [24].

Security questions use a recall mechanism which causes memorability issues. More than 33% of the survey population stated that they use security questions for password reset more than a year after originally setting them. As the time duration increases, it declines the process of memory retention, and users find it difficult to recall their answers. We promote the use of recognition in place of recall to boost memorability with an innovative theme-based approach.

6.2 Proposed Design

We propose a theme-based authentication mechanism relying on the proven efficiency and effectiveness of graphical passwords and the advantages of additional audio input, thus improvising memory association strengths [25]. We use graphical and sound authentication techniques as a part of the theme. Previous studies have shown that users remember images more vividly than text-based schemes. They can recall their graphical password with more 90% accuracy [26]. Although use of graphics aid in memorability, an increase in visual information can cause information overload. A study by Brewstern states that an integrated display of graphics and audio can overcome this information overload [27]. Making an association with images and sounds can improve the efficiency of memory recall (Figure 18).

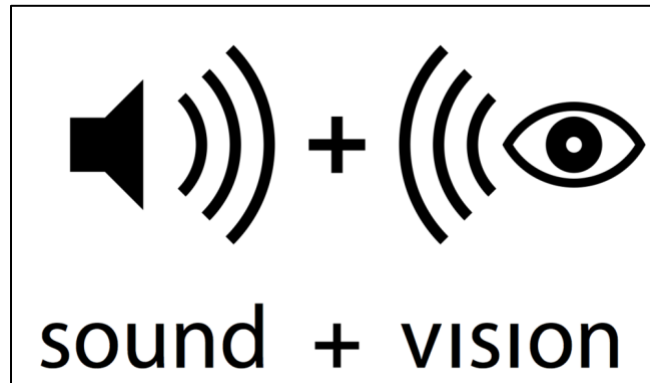


Figure 18: Associating Images with Sound

The proposed theme-based approach uses system generated themes and does not rely on personal information of the user and hence can avoid social engineering attacks. Since it is a knowledge-based authentication mechanism, there are no additional hardware

or software costs associated. The novel approach looks promising and user-friendly since user has a choice to select the theme of her choice and establish an association.

6.2.1 Registration Phase

1. A user registers on the website and provides her username and password. After inputting her details, she is guided towards the fallback authentication setup.
2. The user is provided with a set of predefined themes. This set of predefined themes is standard for all users registering on the site. The user selects a theme of her choice. Themes can be of general topics such as holidays, cartoons, technology, sci-fi etc.
3. The user is then provided with a set of about 10-15 images based on that particular theme. She can select one or multiple images of her choice from the set.
4. After the user selects the images, she is directed towards a set of sound clips, and the user selects a sound clip that can help her relate to the images. Grouping semantically similar objects can invoke the associative memory of the user.
5. The user sets up her theme, which consists of a theme name, set of images and a sound clip. The fallback registration process is complete once the user defines her theme.

The aim of keeping a theme is to establish associations between the objects of the theme can help the user recall these objects in the recall phase. Figure 19 shows the flowchart for registration phase of the theme-based approach.

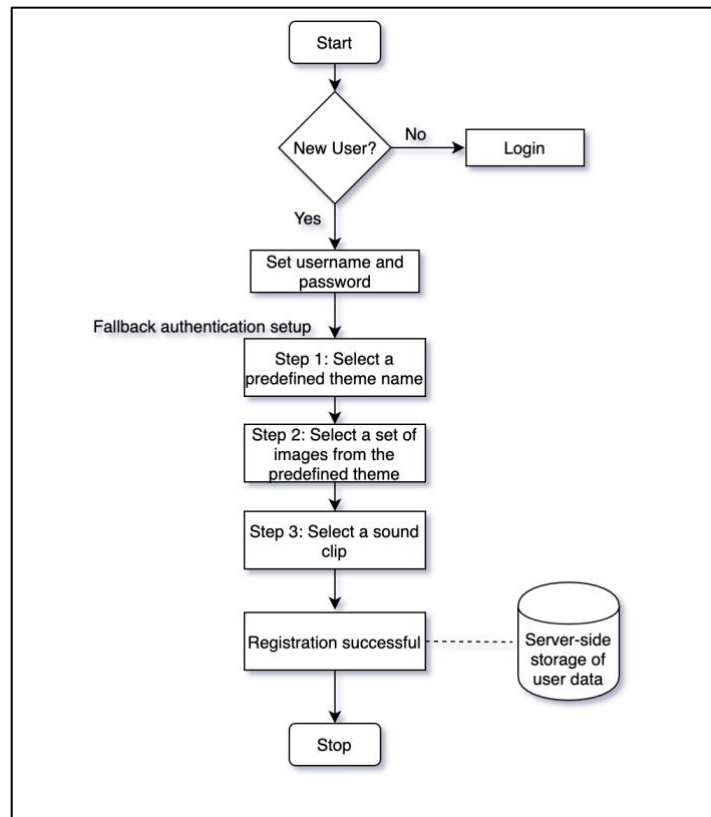


Figure 19: Registration Phase of Theme-based Approach

6.2.2 Recall Phase

1. In case if a user forgets her password, he is redirected to the fallback authentication scheme. He is then provided with a large image set from multiple themes together. The user has to select the images based on the theme she had selected during the registration phase. The order of the images will not be emphasized based on the studies have shown that recalling the sequence of objects also known as *serial recall* declines with time [20].

2. The sound clip selected by the user would be an audio cue for the user to help her invoke associations amongst the images. After correct selection of images, the user is granted access to her account.

The theme names will not be displayed in the recall phase to keep the anonymity of the theme chosen by the user during the registration phase. The number of attempts is restricted to three. The account will get automatically locked if the user selects wrong images. Figure 20 shows the flowchart for recall phase of the theme-based approach.

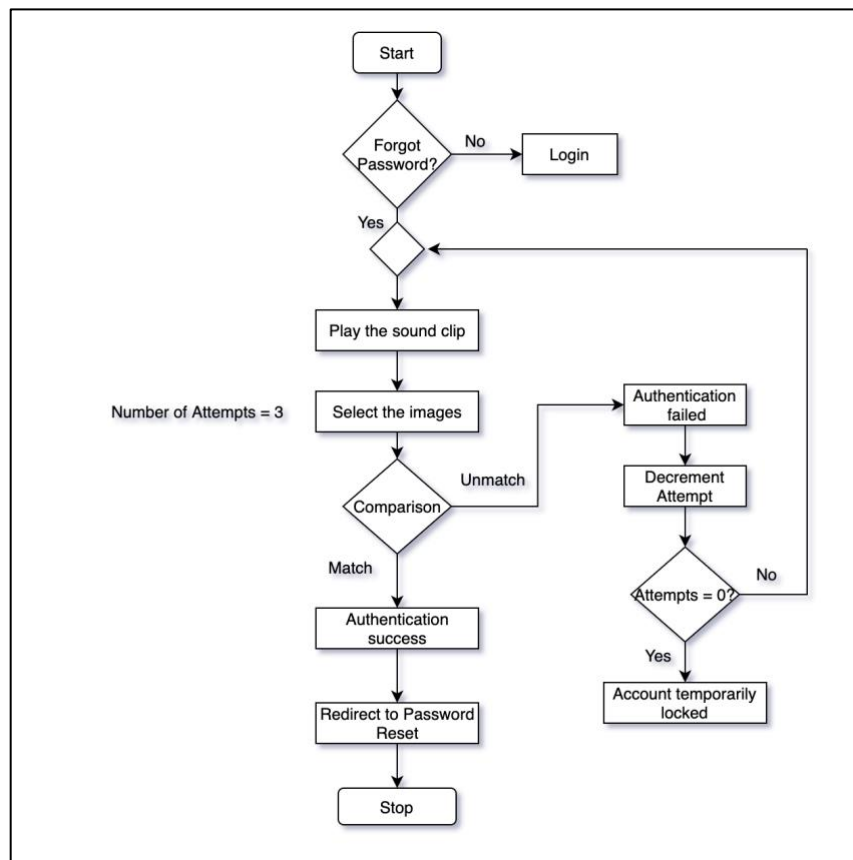


Figure 20: Recall Phase of Theme-based Approach

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 Conclusion

Weak fallback authentication techniques have driven us to explore a unique approach that strikes a balance between usability and security. Our surveys helped us get an understanding of current fallback approaches and what difficulties an end-user faces while utilizing such mechanisms. The memorability experiment successfully confirmed that the effectiveness of recall mechanisms declines with time. We investigated several potential threats to security questions and implemented an attack that exposes the vulnerabilities of security questions and one-time-passwords. We introduce a theme-based approach as an alternative for security questions based on the aspect of recognition. We combine application of visual and sound authentication to improvise the memorability.

7.2 Future Work

There is a need for additional investigation in fallback authentication techniques, as well as more reliable ways of performing a password recovery. We would also like to promote improvement in the usability of security questions by adhering to strict rate-limiting of answers and allowing users to view and change their responses after regular intervals. Future work for the proposed theme-based approach includes adding more

features and more objects to the themes to expand the answer space and make it more secure.

An experimental comparison between the existing security question mechanisms and the proposed approach should be studied to perceive its usability analysis. There is not yet a notable deployment of graphical techniques, though having usability advantages over text-based methods. The proposed approach has the potential to substitute security questions; and therefore, we encourage additional research in graphical and sound authentication techniques.

Appendix A: Screening Survey

What is your age?

- ☐ 18-24 years
- ☐ 25-34 years
- ☐ 35-44 years
- ☐ 45-54 years
- ☐ 55-64 years
- ☐ 65 or older

What is your gender?

- ☐ Male
- ☐ Female
- ☐ Non-binary
- ☐ Other

What is your highest education level?

- ☐ High-school student
- ☐ High-school graduate
- ☐ Associate degree
- ☐ Bachelor's degree
- ☐ Graduate and professional degree (Masters, Doctorate, etc.)
- ☐ Other _____

Which of the following describes your primary occupation?

- ☐ Administrative Support (e.g., secretary, assistant)
- ☐ Art, Writing, or Journalism (e.g., author, reporter, sculptor)
- ☐ Business, Management, or Financial (e.g., manager, accountant, banker)
- ☐ Legal (e.g., lawyer, paralegal)
- ☐ Medical (e.g., doctor, nurse, dentist)
- ☐ Computer Science and Engineering or IT Professional (e.g., programmer, IT consultant)
- ☐ Engineer in another field (e.g., civil or bioengineer)
- ☐ Service (e.g., retail clerk, server)
- ☐ Skilled Labor (e.g., electrician, plumber, carpenter)
- ☐ College Student
- ☐ Graduate Student
- ☐ Unemployed
- ☐ Retired
- ☐ Other _____

Have you ever answered security questions for password reset?

- ☐ Yes
- ☐ Maybe
- ☐ No

If Yes, can you recall a security question you answered recently?

Did security questions help you log back to your account?

- ☐ Always
- ☐ Most of the time
- ☐ Sometimes
- ☐ Never

Appendix B: Security Questions Survey

To what extent do you agree or disagree that someone might try to break into your primary personal email account using your security questions?

- ☐ Strongly Agree
- ☐ Agree
- ☐ Somewhat agree
- ☐ Neither agree nor disagree
- ☐ Somewhat disagree
- ☐ Disagree
- ☐ Strongly disagree

To what extent do you agree or disagree with this statement: “Security questions have poor security.”

- ☐ Strongly Agree
- ☐ Agree
- ☐ Somewhat agree
- ☐ Neither agree nor disagree
- ☐ Somewhat disagree
- ☐ Disagree
- ☐ Strongly disagree

What fallback authentication method you prefer presupposing you forget the password?

- ☐ Email Verification
- ☐ Short message service (SMS) verification
- ☐ Provide reset code to trusted contacts
- ☐ Passcode/keys
- ☐ Security questions

Why do you prefer the selected method?

Do you prefer system Built-in security questions or User-generated (open end) security questions?

- ☐ Built-in (Answer the given system-generated security questions)
- ☐ User-generated (Provide your own security questions and answers)
- ☐ Neither
- ☐ Both

Why do you prefer system Built-in security questions?

Why do you prefer User-generated (open end - provide your own questions and answers) security questions?

Do you remember the answers you have provided to security questions?

- ☐ Definitely yes
- ☐ Probably yes
- ☐ Probably not
- ☐ Definitely not

If No, what is the reason to forget the answers provided to security questions?

- ☐ Answered it long back
- ☐ Answered it incorrectly
- ☐ Didn't expect to answer it
- ☐ Other _____

Do you share your security question answers with others?

- ☐ Always
- ☐ Most of the time
- ☐ Sometimes
- ☐ Never

Do you store answers to your security questions?

- ☐ Yes – Electronically (On phone, Computer, etc.)
- ☐ Yes - On Paper
- ☐ No
- ☐ Other _____

Do you provide simple/easy answers to security questions so that they are easy to remember(memorable)?

- ☐ Always
- ☐ Most of the time
- ☐ Sometimes
- ☐ Never

Do you prefer if a hint is provided with security questions?

- ☐ Yes
- ☐ No

If Yes, why do you prefer a hint?

If No, why don't you prefer a hint?

Do you provide correct (truthful) answers to security questions?

- ☐ Yes
- ☐ No

If No, why do you provide untruthful/incorrect answers?

- ☐ Answer is easy to remember
- ☐ Answer is harder to guess
- ☐ Don't want to share the right answer
- ☐ Did not understand the question
- ☐ Other _____

How often do your answers to security questions change over time? (e.g., "What is your favorite movie?")

- ☐ Always
- ☐ Most of the time
- ☐ Sometimes
- ☐ Never

How many attempts do you need to answer security questions correctly to log back in?

- ☐ 1
- ☐ 2-3
- ☐ More than 3

What is the time duration between setting up security questions and using them for password reset?

- ☐ Within the first 3 months
- ☐ 3 – 6 Months
- ☐ 6 – 12 Months
- ☐ More than a year

Do you have any views regarding the usability of security questions?

Bibliography

1. W. Yang, N. Li, O. Chowdhury, A. Xiong and R. Proctor, "An empirical study of mnemonic sentence-based password generation strategies," in *Proceedings of 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1216-1229, Vienna, Austria, October 2016.
2. J. Bonneau, E. Bursztein, I. Caron, R. Jackson and M. Williamson, "Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google," in *Proceedings of 24th international conference on world wide web*, pp. 141-150, Florence, Italy, May 2015.
3. A. Javed, D. Bletgen, F. Kohlar, M. Dürmuth and J. Schwenk, "Secure fallback authentication and the trusted friend attack," in *Proceedings of 2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pp. 22-28, Madrid, June 2014.
4. N. Gelernter, S. Kalma, B. Magnezi and H. Porcilan, "The password reset MitM attack," in *Proceedings of 2017 IEEE Symposium on Security and Privacy (SP)*, pp. 251-267, San Jose, CA, May 2017.
5. T. Mohamed, "Security of Multifactor Authentication Model to Improve Authentication Systems," *Information and Knowledge Management Journal*, vol. 4, no. 6, pp. 81-86, 2014.
6. S. Garfinkel, "Email-based identification and authentication: An alternative to PKI?," *IEEE Security & Privacy*, vol. 1, no. 6, pp. 20-26, December 2003.
7. D. Parsons, H. Ryu and M. Cranshaw, "A study of design requirements for mobile learning environments," in *Proceedings of 6th IEEE International Conference on Advanced Learning Technologies (ICALT)*, pp. 96-100, Kerkrade, Netherlands, July 2006.
8. M. Zviran and W. J. Haga, "A comparison of password techniques for multilevel authentication mechanisms," *The Computer Journal*, vol. 36, no. 3, pp. 227-237, January 1993.
9. M. Just and D. Aspinall, "Personal choice and challenge questions: a security and usability assessment," in *Proceedings of 5th Symposium on Usable Privacy and Security*, pp. 1-11, Mountain View, CA, July 2009.

10. A. Hang, A. D. Luca, M. Smith, M. Richter and H. Hussmann, "Where have you been? using location-based security questions for fallback authentication," in *Proceedings of 11th Symposium on Usable Privacy and Security*, pp. 169-183, Ottawa, Canada, July 2015.
11. A. Senarath, N. Arachchilage and B. Gupta, "Security strength indicator in fallback authentication: Nudging users for better answers in secret question," *International Journal for Infonomics*, vol. 9, no. 4, pp. 533-537, January 2017.
12. N. Micallef and M. Just, "Using avatars for improved authentication with challenge questions," in *Proceedings of 5th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE)*, pp. 121-124, France, August 2011.
13. H. Gao, X. Liu, S. Wang, H. Liu and R. Dai, "Design and analysis of a graphical password scheme," in *Proceedings of 4th International Conference on Innovative Computing, Information and Control (ICICIC)*, pp. 675-678, Kaohsiung, December 2009.
14. S. Akula and V. Devisetty, "Image based registration and authentication system," [Online]. Available: <https://pdfs.semanticscholar.org/c3f0/8f67e50b880ecdb24d4f4a5c9578ea4d378c.pdf> [Accessed: April 2020].
15. S. Almuairfi, P. Veeraraghavan and N. Chilamkurti, "IPAS: implicit password authentication system," in *Proceedings of 2011 IEEE workshops of international conference on advanced information networking and applications*, pp. 430-435, Singapore, March 2011.
16. D. Ramsay, I. Ananthabhotla and J. Paradiso, "The Intrinsic Memorability of Everyday Sounds," in *Proceedings of 2019 Conference on Immersive and Interactive Audio*, pp. 87-97, York, UK, March 2019.
17. A. Ullah, H. Xiao, T. Barker and M. Lilley, "Graphical and text-based challenge questions for secure and usable authentication in online examinations," in *Proceedings of 9th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 302-308, London, December 2014.
18. M. Just and D. Aspinall, "Challenging Challenge Questions: An Experimental Analysis of Authentication Technologies and User Behaviour," *Policy & Internet Academic Journal*, vol. 2, no. 1, pp. 99-115, April 2010.
19. G. Scoville, "Good Security Questions," [Online]. Available: <http://goodsecurityquestions.com/> [Accessed: April 2020].

20. P. Noble and R. Shiffrin, "Retrieval processes in recognition and cued recall," *Journal of Experimental Psychology: Learning, Memory, and Cognition*, vol. 27, no.2, pp. 384-413, March 2001.
21. D. Sukhram and T. Hayajneh, "KeyStroke logs: Are strong passwords enough?," in *Proceedings of 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, pp. 619-625, New York, October 2017.
22. Y. Lee, N. Kim, H. Lim, H. Jo and H. Lee, "Online banking authentication system using mobile-OTP with QR-code," in *Proceedings of 5th IEEE International Conference on Computer Sciences and Convergence Information Technology*, pp. 644-648, Seoul, November 2010.
23. R. Budiu, "Memory Recognition and Recall in User Interfaces," [Online]. Available: <https://www.nngroup.com/articles/recognition-and-recall/> [Accessed: April 2020].
24. N. Micallef and N. Arachchilage, "Changing users' security behavior towards security questions: A game based learning approach," in *Proceedings of 2017 Military Communications and Information Systems Conference (MilCIS)*, pp. 1-6, Canberra, November 2017.
25. J. Liddell, K. Renaud and A. Angeli, "Authenticating users using a combination of sound and images," [Online]. Available: https://www.researchgate.net/publication/267553796_Authenticating_users_using_a_combination_of_sound_and_images [Accessed: April 2020].
26. D. Weinshall and S. Kirkpatrick, "Passwords you'll never forget, but can't recall," in *Proceedings of 2004 Conference on Human factors in computing systems*, pp. 1399-1402, Vienna, Austria, April 2004.
27. S. Brewster, "Using non-speech sound to overcome information overload," *Displays*, vol. 17, no. 3-4, pp. 179-189, May 1997.