OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

UNDERSTANDING SMARTPHONE SENSOR AND APP DATA FOR ENHANCING THE SECURITY OF SECRET QUESTIONS BASED AUTHENTICATION SYSTEM

V S Karvande[1], Shailesh Shinde[2]

Asst. Prof. CSE Department, Everest Collage of Engineering and Technology, Aurangabad[1]

Student, CSE Department, Everest Collage of Engineering and Technology, Aurangabad[1]

shindeshailesh78@gmail.com[2]

Abstract: **At present with increasing popularity of online shopping Debit or Credit card fraud. Personal information security is major concerns for customers, merchants and banks specifically in the case of Card Not Present. Many web applications provide secondary authentication methods i.e., secret questions (or password recovery questions), to reset the account password when a users login fails. Today's prevalence of smart phones has granted us new opportunities to observe and understand how the personal data collected by smart phone sensors and apps can help create personalized secret questions without violating the users' privacy concerns. We also provide a secure system for barcode based visible light communication for online payment system using image stenography methodology. We present a Secret-Question based Authentication system, called "Secret- QA" that creates a set of secret questions on the basis of peoples smart phone usage. We develop a prototype on Android smart phones, and evaluate the security of the secret questions by asking the acquaintance /stranger who participate in our user study to guess the answers with and without the help of online tools meanwhile we observe the questions reliability by asking participants to answer their own questions.**

I INTRODUCTION

The blank-filling secret questions are dominant as the mainstream authentication solution, especially in web and email authentication systems, despite the criticism on its security and reliability. Guessing attacks by acquaintance and stranger. The security of secret questions for authentication was studied by Zviran and Haga in 1990 [2], which indicated that the answers of 33% questions can be guessed by the "significant others" who were mainly participants spouses (77%) and close friends (17%). Another similar study was conducted by Poddet al, which revealed a higher rate of successful guessing (39.5%). A recent study showed that even an open question written by the user himself was still vulnerable to the guessing attacks launched by his acquaintance [4]. On the other hand, strangers can be more sophisticated than ever to launch the guessing attacks, as they can access the user's personal his-tory through online social networks (OSN) or other public online tools. Therefore, the statistical guessing has become an effective way to compromise a few personal "secret" questions (e.g., "Where were you born?", "What is the name of your high school?"). Poor reliability of secret questions in real world. Regarding the reliability, a secret question should be memory-wise effortless for users. However, todays mainstream secret question methods fail to meet this requirement. A recent study re-veiled that nearly 20% users of four famous webmail providers forgot their answers within six months [4]. Moreover, dominant blank filling secret questions with case sensitive answers require the perfect literally matching to the set answer which also contributes to its poor reliability.

II OBJECTIVES

- To design a user authentication system with a set of secret questions created based on the data of users short-term smart phone usage.
- No need to memories password
- Its provide security.
- Privacy protection.
- User's short term.
- Real word secrete question Reliability.

III PROBLEM STATEMENT

To developed a prototype on Android smart phones, and evaluate the security of the secret questions by asking the acquaintance/stranger who participate in our user study to guess the answers with and without the help of online tools meanwhile we observe the questions reliability by asking participants to answer their own questions.

3.1.1 Goals and objectives

To design a user authentication system with a set of secret questions created based on the data of users short-term smartphone usage.

3.1.2 Statement of Scope

This work is to study whether using smartphone sensor/ app data is helpful for secret-question based secondary authentication.

People like students have the necessary experience on setting and answering secret questions and they use smartphones and online tools every day.

The secret questions related to motion sensors, calendar, app installment, and part of legacy apps (call) have the best performance in terms of memorability and the attack resilience, which outperform the conventional secret-question based approaches that are created based on a users long-term his-tory/information.

In this system, our research provides a gridline that shows. Which sensors/app data and which type of question are suitable for devising secret question.

This implies improved security for such secret questions

Cost Estimate

Costs of the getting knowledge is depends on the resources and efforts needed for the development of the system. The cost of the project is approximately 20,000.

Line of Code (LoC)

Estimating LOC for this project is difficult at estimation stages this project is of research or innovative type project. Average estimation of this project is to 9k to 10k line of code.

Cost of project C = N*Cp

C = 4*5000 C = 20,000

The cost of the project is approximately 20,000

IV USAGE SCENARIO

1. *The User-event Extraction Scheme:*

Today's smart phones are typically equipped with a plethora of sensors and apps which can capture various events related to a users daily activities, e.g., the accelerometer can record the users sports/motion status without consuming excessive battery.

Selection of sensors/apps. In the user-event extraction scheme, Secret-QA selects a lists of sensors and apps for extracting the user activities, including: Given the designated sensors and apps for building the authentication system, we develop a Secret-QA client app called Event Log to extract the features for question generation. Secret-QA server.

A trusted server is used as the auditor, which can also provide the user authentication service even if the phone is not available.

Participant Recruitment:

We count the number of calls (or SMS) from/to every contact, or the number of times an app is used by a participant, for creating the frequency-based question, e.g., No. 34 Who was your most frequent contact last week?. If there are more than one most frequent contacts or most frequently used apps, any answer within these candidates is considered correct. Answers to blank-filling questions For each blank-filling question, we have a default correct answer that is set by our system, as well as an answer input by the participant in the memory test.

Reliability and resilience to attacks:

We set the threshold of easy-to-remember questions to be 80% for both true/false and multiple choice questions i.e., 80% participants to correctly answer the question, according to the threshold used for traditional web-mail secret questions. A random guessing attack has a success rate of 50% and 25% for true/false and multiple choice (one of four options) questions, respectively percent.

Report generation:

We present a Secret-Question based Authentication system, called Secret-QA, and conduct a user study to understand how much the personal data collected by smart phone sensors and apps can help improve the security of secret questions without violating the users privacy. We create a set of questions based on the data related to sensors and apps, which reflect the users short-term activities and smart phone usage. We measure the reliability of these questions by asking participants to answer these question, as well as launching the acquaintance/stranger guessing attacks with and without help of online tools, and we are con-side ring establishing a probabilistic model based on a large scale of user data to characterize the security of the secret questions.

V ARCHITECTURAL DESIGN

The reliability of a secret question is its memorability the required effort or difficulty of memorizing the correct answer. Without a careful choice of a blank filling secret question, a user may be declined to log in, because he cannot remember the exact answer that he provided, or he may misspell the input that requires the perfect literally-matching to the correct answer. We design a user

authentication system with a set of secret questions created based on the data of users short-term smart phone usage. We evaluated the reliability and security of the three types of secret questions (blank-filling, true/false, and multiple-choice) with a comprehensive experiment in-evolving 88 participants. The experimental results show that the combination of multiple lightweight true-false and multiple choice questions required less input effort with the same strength provided by blank-filling questions. We evaluate the usability of the system, and find that the Secret-QA system is easier to use than those existing authentication system with secret questions based on users long-term historic data.

Modules

1. *The User-event Extraction Scheme*

Today's smart phones are typically equipped with a plethora of sensors and apps which can capture various events related to users daily activities, e.g., the accelerometer can record the users sports/motion status without consuming excessive battery. Selection of sensors/apps. In the user-event extraction scheme, Secret-QA selects a lists of sensors and apps for extracting the user activities, including: Given the designated sensors and apps for building the authentication system, we develop a Secret-QA client app called Event Log to extract the features for question generation. Secret QA server. A trusted server is used as the auditor, which can also provide the user authentication service even if the phone is not available.

2. *Participant Recruitment*

We count the number of calls (or SMS) from/to every contact, or the number of times an app is used by a participant, for creating the frequency-based question, e.g., No. 34 Who was your most frequent contact last week?. If there are more than one most frequent contacts or most frequently used apps, any answer within these candidates is considered correct. Answers to blank-filling questions. For each blank-filling question, we have a default correct answer that is set by our system, as well as an answer input by the participant in the memory test.

3. *Reliability and resilience to attacks*

We set the threshold of easy-to-remember questions to be 80% for both true/false and multiple choice questions i.e., 80% participants to correctly answer the question, according to the threshold used for traditional webmail secret questions. A random guessing attack has a success rate of 50% and 25% for true/false and multiple choice (one of four options) questions, respectively percent

4. *Report generation*

We present a Secret-Question based Authentication sys-tem, called Secret-QA, and conduct a user study to understand how much the personal data collected by smart phone sensors and apps can help improve the security of secret questions without violating the users privacy. We create a set of questions based on the data related to sensors and apps, which reflect the users short-term activities and smart phone usage. We measure the reliability of these questions by asking participants to answer these question, as well as launching the acquaintance/stranger guessing attacks with and without help of online tools, and we are considering establishing a probabilistic model based on a large scale of user data to characterize the security of the secret questions.

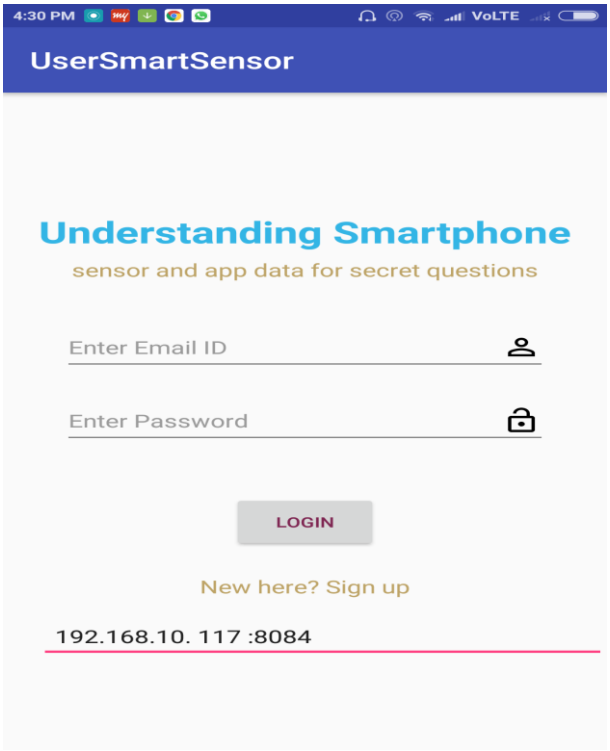

Figure 1 User Smart Sensor Application

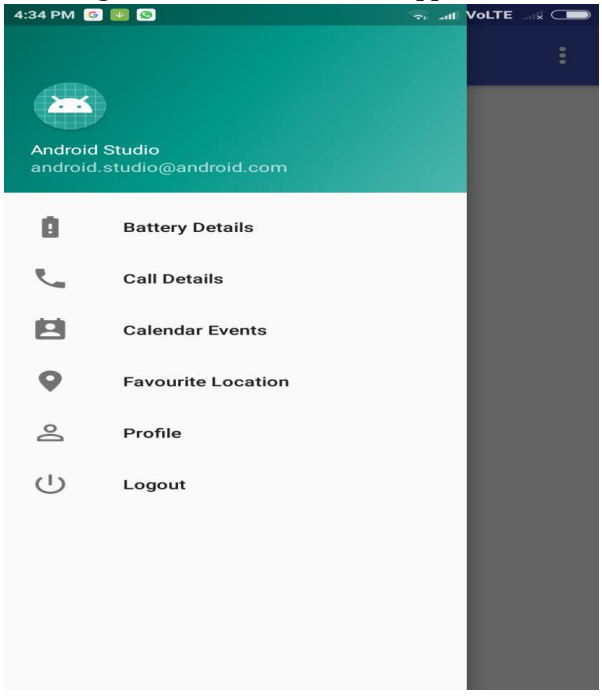

Figure 2 Mobile Details

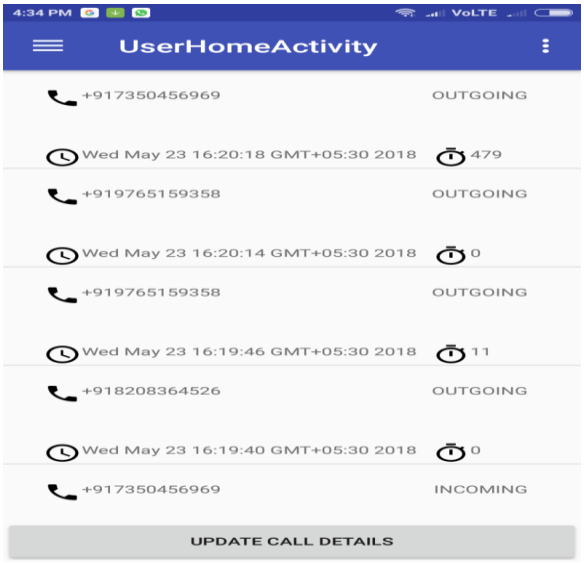

Figure 3 Update Call Details

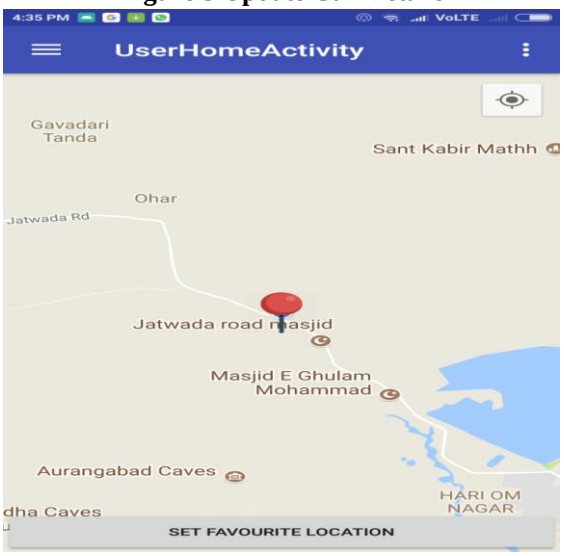

Figure 4 Set favorite Location

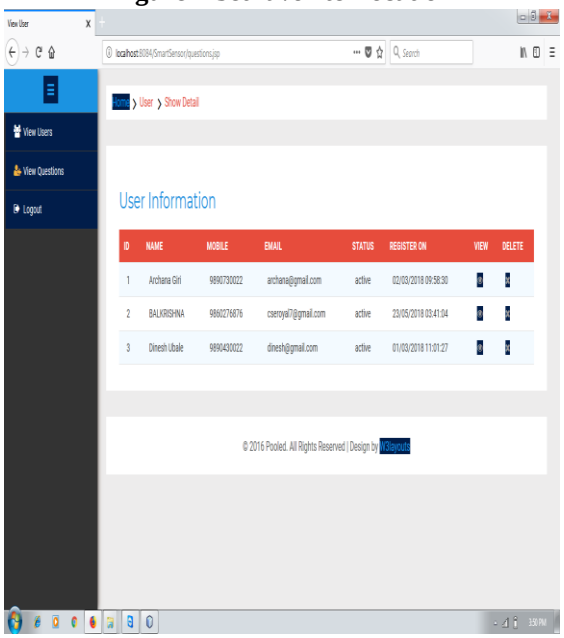

Figure 5 User Details

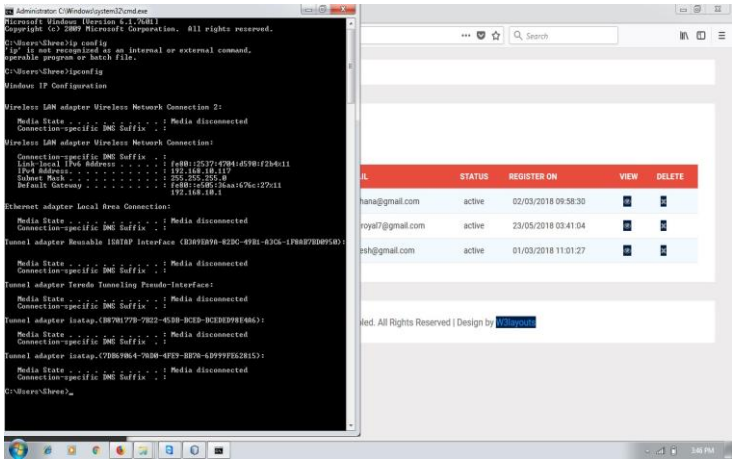

Figure 5 Check ipv4 Address

VI CONCLUSION

We Proposed a Secret-Question based Authentication framework, called ”Mystery QA”, and lead a client concentrate to see how much the individual information gathered by cell phone sensors and applications can help enhance the security of mystery inquiries without damaging the clients’ protection. We make an arrangement of inquiries in light of the information identified with sensors and applications, which mirror the clients’ transient exercises and cell phone utilization. We measure the dependability of these inquiries by requesting that members answer these inquiry, and in addition propelling the associate/more peculiar speculating assaults with and with-out help of online apparatuses, and we are thinking about setting up a probabilistic model in light of a substantial size of client information to describe the security of the mystery questions. In our test, the mystery questions identified with movement sensors, date-book, application portion, and part of inheritance applications (call) have the best execution as far as memorability and the assault flexibility, which beat the ordinary mystery question based methodologies that are made in light of a client’s long haul history/data.

REFERANCES

[1]R. Reeder and S. Schechter, “When the password doesn’t work: Secondary authentication for websites,” *S & P., IEEE*, vol. 9, no. 2, pp. 43–49, March 2011.

[2] M. Zviran and W. J. Haga, “User authentication by cognitive passwords: an empirical assessment,” in *Information Technology, 1990.’Next Decade in Information Technology’, Proceedings of the 5th Jerusalem Conference on (Cat. No. 90TH0326-9)*. IEEE, 1990, pp. 137–144.

[3] J. Podd, J. Bunnell, and R. Henderson, “Cost-effective computer security: Cognitive and associative passwords,” in *Computer-Human Interaction, 1996. Proceedings. Sixth Australian Conference on*. IEEE, 1996, pp. 304–305.

[4] S. Schechter, A. B. Brush, and S. Egelman, “It’s no secret. measuring the security and reliability of authentication

via secret questions," in *S & P., IEEE*. IEEE, 2009, pp. 375–390.

[5] S. Schechter, C. Herley, and M. Mitzenmacher, "Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks," in *USENIX Hot topics in security*, 2010, pp. 1–8.

[6] D. A. Mike Just, "Personal choice and challenge questions: A security and usability assessment," in *SOUPS.*, 2009.

[7] A. Rabkin, "Personal knowledge questions for fallback authentication: Security questions in the era of facebook," in *SOUPS*. ACM, 2008, pp. 13–23.

[8] J. C. Read and B. Cassidy, "Designing textual password systems for children," in *IDC.*, ser. IDC '12. New York, NY, USA: ACM, 2012, pp. 200–203.

[9] H. Ebbinghaus, *Memory: A contribution to experimental psychology*. Teachers college, Columbia university, 1913, no. 3.