Short-Term History Based Authentication Using Smartphone Sensors and Apps

[1]Anjana K. V., [1]Gopika Vinod,[1]Aneena Shaju, [1]Appu K. Asok, [2]Ancy A., [3]Sangeetha Srinivas, [4]Dr. SuvanamSasidharBabu
[1]PG students, [2]Assistant Professor, [3]Associate Professor,[4]Professor
Department of CSE
SNGCE, Kadayiruppu

Abstract

Secrete-QA could be a security primarily based application. A security question is asked once the user fails to login or forgets his/her password and to reset the password. A security question could be a secondary authentication, but these queries is guessed simply by an admirer or exposed to a strangers who might recognize our personal info like friends, relations or those that will access our personal info through public on-line tools. We will build these security queries additional customized by using the privilege of accessing our Smartphone sensors and apps while not affecting the user's privacy. Three types of questions are generated that is, Yes/No questions, Multiple Choice questions and WH questions. An android app is created for the frequent updating of the Smartphone data and questions are asked in the web part using this updated data.The questions are generated by considering the legacy apps, GPS, calendar, app details etc.These have the mostmemorability to the users and high robustness to attacks.

Keywords *Secret-QA, Secondary Authentication, Public online tools, Legacy apps.*

INTRODUCTION

Security question is used as an authenticator by banks, wireless providers, social networks Institution's use of security question as a supplement to customer signature records. In 2000s, security questions came into widespread use on the internet. As a form of self-service password reset, security questions have reduced information technology help desk costs. By allowing the use of security questions online, they are rendered vulnerable to keystroke logging attacks. In addition,whereas human customer service representative may be able to cope with inexact security answers appropriately, computers are less [1]. As such users must remember the exact spelling and sometimes even case of the answers they provide, which poses the threat that more answers will be written down, exposing them to physical theft.

Due to the commonplace nature of the social media may of the older security questions are no longer useful or secure. It is important to remember that a security question is just another password. Therefore, a security question should not include any information readily available ion social media websites, while remaining simple, memorable, difficult to guess, and constant over time. Many have questioned the usefulness of security questions. Security specialists points out that since they are public facts about a person, they are easier to guess for hackers than passwords. Users that know this create fake answers to the questions, then forget the answers, thus defeating the purpose and creating an inconvenience not worth the investment.

Most of the webmail providers rely on personal questions as the secondary authentication secrets used to reset account passwords. The security of these questions has received limited formal security, almost all of which predates webmail. Most of the security questions are blank filling questions to improve their reliability [2]. These type of questions are created based on the long term history of the user. Long term history is the information about the user which doesn't change for months/years (example:" What is the name of your favorite teacher?")[3]. These kind of questions may lead to poor security and reliability. It is because of that these kind of questions can be easily answered by the users friends, relatives or people who know them closely[3]. The security of a question depends on the assumption: "A user's long term personal history is only known by the user himself"[1].

However this assumption does not hold any validity. Moreover that a stranger can easily crack the password by figuring out the answers leaked from public user profiles in online social networks or search engines.

In the current scenario Smartphone's are used for the most of the online purposes because of its ease of use and the Smartphone provide a rich source of user's personal information related to his short-term history. These kind of personal data I collected by the Smartphone sensors and apps[4]. By considering a person's Smartphone usage for generating a security question we have to face a lot of privacy issues .But by accessing the short term history the security question will become more reliable and more secure. The reasons for this reliability and security are

- The short term history will be less exposed to a stranger or acquaintance when compared to the long term history.
- Because of the frequent variations in the events will make the questions more secure as it has validity for a short period of time
- Moreover that the memorability of the short term history will be more .It is easier to memorize a short term data than a long term data. The reliability of the security question is its memorability. In this paper we are presenting a Security based Authentication System.SecretQA is implemented as an android app which take the advantage of the data of the Smartphone sensors and apps for generating a set of security questions. These questions are generated used on the Smartphone usage. The rest of the paper gives an idea about the whole application and how it get implemented.

BACKGROUND AND RELATED WORKS

In the current scenario blank filling questions are dominant in the authentication solution. Most of the web and email authentication system uses blank filling questions as the secondary authentication.

- The guessing on a security question based on long term history will be easy for a stranger to crack.

- Poor reliability of the security question. In the reliability context the secret question with case sensitive answers require the perfect literally matching to the set answer, which contributes to its poor reliability.
- The recent proposals are the usage of Smartphone sensors and apps for creating a short term security question.
- The Secret-QA creates a set of questionsbased on the Smartphone usage and divide these questions into differenttypes of questions such as blank filling questions, Yes/No questions and Multiple choice

Questions. As we are using different types of question the user has the privilege to choose the questions. Yes /No and Multiple choice Questions are light weighted question ,because answering the above type of questions will be easier for the user when compared to the blank filling questions.

SYSTEM OVERVIEW

EXISTING SYSTEM

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. Many websites and OSN are using these methods to improve the security.

In current system the websites will provide predefined questions and the user must answer these questions in the time of registration. The website will store these questions and its corresponding answers in its database[5]. If the user forgot his password and tries to access his/her account. The website will produce the questions that he/she answered during the time of registration. If the user answers correctly he/she can change the password and access the account otherwise that user will be rejected.

PROPOSED SYSTEM

Smartphone has become one’s most indivisible device of recording his life, this study presents a user authentication system Secret-QA to review on however ones’ short-run history will edges the safety and dependableness of secret queries. This study evaluate the attack strength of employing a combination of the many light-weight queries (true/false, multiple-choice) rather than using the blank-fillings, so as to strike a balanced exchange between security (and reliability) and usefulness [1].

The Secret-QA system consists of 2 major elements, particularly the user-event extraction theme and therefore the challenge-response protocol. The user-event extraction part can gather the Smartphone device and app knowledge from the user’s smart phone. The challenge response protocol can produce totally different queries and corresponding answers supported the gathered knowledge. If the user answers properly he will access to his account otherwise he are rejected.

This new system will improve the security of the secret questions because the answers for that questions will be easy to remember and hard to guess. So attacking by acquaintances and strangers can be reduced.

SYSTEM DESIGN

System Design is the process of defining the architecture, modules, interfaces, and data for a system to satisfy specified requirements. Systemdesign could be seen as the application of system theory to product development. There is some overlap with the disciplines of systems analysis, system architecture and systems engineering[6] .It is a transaction from user-oriented documents to document oriented programmers or database personnel, it emphasis on translating performance specification into design specification and involves conceiving, planning and then carrying out the plan by generating the necessary reports and outputs.

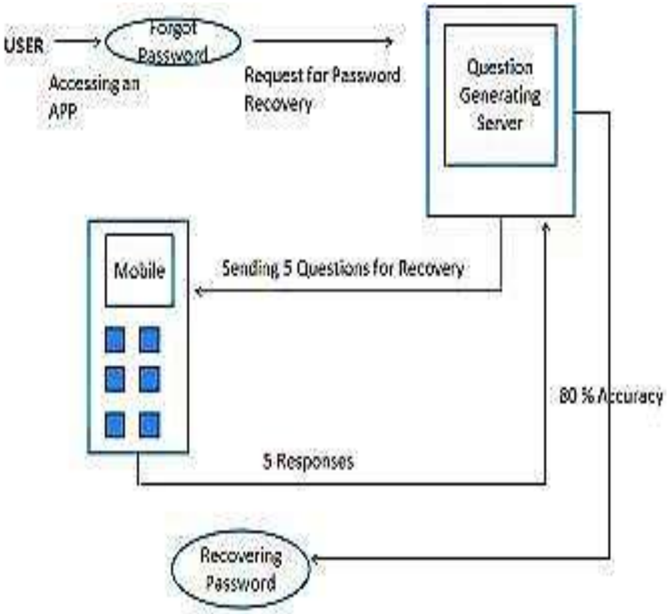
USER
Forgot Password
Accessing an APP
Request for Password Recovery
Question Generating Server
Mobile
Sending 5 Questions for Recovery
80 % Accuracy
5 Responses
Recovering Password

***Fig. 1** Password Recovery*

MODULE

User Event Extraction

User event extraction in Secret-QA is done by creating an android app which extracts the details of the smartphone usage that is in the user event extraction the information from the legacy apps, installed app details, calendar events, GPSdetails, call details, SMS details, contact details are extracted and frequently updated to the database from fig.1.

- The events get frequently updated to maintain the short-term history.
- The events get updated each time when the user uses the app for event extraction.
- The app collect details such as call details, SMS details, contact details etc.

Question Generation

Secret-QA generates a set of questions based on the extracted events. The questions are of three types

- Blank Filling Questions
- Yes/No Questions
- Multiple Choice questions

Blank Filling Questions

Blank filling questions has the highest reliability given below are the examples of some blank filling questions

1. Which is the last installed app?
2. Which is the app you updated yesterday?
3. Whom did you called last?
4. What is you phones battery percentage?
5. Who is your most frequent SMS contact?

Multiple Choice Questions

Multiple choice questions provide 44 choices along with the question and it will be much more easier for the user to answer the questionexample: “Who was you most frequent contact last week?”. If there is more than one most frequent contact or most frequently used apps, any answer within these candidates is considered correct.

Yes/No Questions

The Yes/No questions takes information about the location details, calendar events, battery details, SMS details etc. Its answer will be either true or false.For example" Do you call someone yesterday?"

FEATURES

The application first ask the user to select the type of the question that is, Yes/No or multiple choice or blank filling a set of 5 questions are asked based on the selected type and if the user answer four questions correctly then the user can reset his /her password otherwise the system get blocked for a period of 30 seconds.

- The reliability is increased
- User has the option to select the type of the question
- The issue of memeorability is reduced to a certain extend because of the usage of short term history
- user friendly application

CONCLUSION AND FUTURE WORKS

Secret-QA creates a gaggle of queries supported the data involving sensors and apps, that replicate the users' short activities and smartphone usage. The responsibility of the queries are often measured by asking the participants to answer these queries, furthermore as launching the acquaintance/stranger approximation attacks with and while not facilitate of on-line tools, and are considering establishing a probabilistic model supported an oversized scale of user knowledge to characterize the protection of the key queries. The key queries involving motion sensors, calendar, app installment, and a locality of inheritance apps (call) have the best performance in terms of memorability and conjointly the attack resilience, that beat out the normal secret-question based totally approaches that area unit created supported a user's long-term history/information.

The future work focuses on auto updation of the user events rather than updation at the time of app usage. Including more questions and making the application fully app based rather than generating the question at the web.

REFERENCES

1. Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Question IEEE Transactions on Mobile Computing (Volume: 16, Issue: 2, Feb. 1 2017).
2. Selective checkpointing for minimizing recovery energy and efforts of smartphone apps Green and Sustainable Computing Conference (IGSC), 2017 Eighth International
3. WebLogger: Stealing your personal PINs via mobile web application Wireless Communicationsand Signal Processing (WCSP), 2017 9th International Conference
4. Mariŏcagalj, C toniperkoví, C marinbugarí,"Timing attacks on cognitive authentication schemes", *ieee transactions on informationforensics and security*, vol. 10, no. 3, march 2015.
5. Analysis of various authentication schemes for passwords using images to enhance network security through online services P. SahayaSuganya Princes; J. Andrews 2017 International Conference on Information Communication and Embedded Systems (ICICES) 2017
6. Password guessing time based on guessing entropy and long-tailed password distribution in the large-scale password dataset, Anti-counterfeiting, Security, and Identification (ASID), 2017 11th IEEE International Conference