International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 7 Issue: 4 01 - 03

Secret Questions based Authentication System for Android Smartphone

Akash Jagtap
Computer Department
Met bhujbal knowledge city,IOE.
Nashik, India
e-mail: Jagtapakash638@gmail.com

Anil Sarwade
Computer Department
Met bhujbal knowledge city,IOE.
Nashik, India
e-mail:sarwadeanil456@gmail.com

Harshal Jhalawat
Computer Department
Met bhujbal knowledge city,IOE.
Nashik, India
e-mail:Jhalawatharshal8@gmail.com

Guide: Mrs.R.V.Chaudhari
Assistant Professor,
Computer Department
Met bhujbal knowledge city,IOE.
Nashik, India
e-mail:Rekha8590@gmail.com

***Abstract*—**We present a android application for enhanced security of password recovery questions.We make use of the sensors available in an basic andorid smartphone to provide security.Many web applications as well as android applications use old and easy to break through questions for password retrieval which can be easily guessed by anyone having zero to very little information about the user.Our system is based on users short term memory.We make use of smartphone sensors and ask questions which are only known to user relying on his short term memory for password retrieval.We present sensor based security questions for password retreival which ultimately increase the security and provide genuine authentication.

Keywords*-Sensor, Authentication, Invasive software, Security, Unauthorized access, Location based reminder , GPS, Mobile Application*

*****

I. INTRODUCTION

Security questions also called as password recovery questions have been widely used as the alternative authentication method for resetting the password when the acutal user credential is forgotten. When ever a user creates an account on any platform he/she needs to choose a set of security questions incase the original credential is forgotten. The user can reset the account's password by answering correctly to the security questions.These questions are usually blank filling questions and short answer questions so that they can be easily memorized by the user.Also these questions are based on users long term knowledge or memory and personal information, (e.g., “What’s the name of your first car?”). However, existing research has shown that such questions are easy to break throug by the attackers or users acquaintance making the systems security poor. Also the user can forget the answers to these long term memory related questions and hence would not be able to access the system.Also a stranger can figure out the answers to the questions by doing little research about the user and getting information from users social media handles like facebook, twitter, instagram etc which is not ideal for the system.Due to the recent prevalence of Smart phone it has provided a rich source of the user’s personal data related to the knowledge of his short-term history, i.e., the data collected by the Smartphone sensors and apps. Is it easy to use the knowledge of one’s short term personal history for creating his secret question.The short-term personal history is less likely to be exposed to a stranger or acquaintance, because the quick changes of an event that a user has experienced within a short term will increase the resilience to guess attacks. This implies improved security for such secret questions.

In this paper, we present a Secret-Question based Authentication system, called “Secret-QA”, taking full advantage of the data of Smartphone sensors and apps without violating any of user's privacy.We design a user authentication system with a set of secret questions created and assembled based on the data of users’ short-term Smartphone usage.

- We evaluated the system security by making use of the multiple types of secret questions like true or false questions (YES/NO), MCQ’s and blank filling questions as well.
- The experimental results show that the mixture of many lightweightYes/No questions and MCQ’s required less amount of input effort with the same strength as compared by blank-filling questions.

- We find that the system is easier to use than those existing authentication system with security questions based on users long-term memory.

II. LITERATURE SURVEY

Designing textual password systemsfor children

This paper was published by J.C Read and B. Cassidy in the year of 2012. This paper shows a system build for designing textual passwords which can be remembered by children and teens.

If the password selection is not done carefully a user may be declined to log into the system and access it in any circumstance. The system uses text as a medium to create passwords that can be easily remembered by children and teens in their early age. Also the paper does not make use of any sensors of the smartphone to create the security questions.

Personal knowledge questions for fallback authentication Security questions in the era of facebook:

This paper was published by A. Rabkin in the year 2008.

Almost all online websites, computer applications, android applications, that uses user-specific accounts make use of passwords to verify that a user attempting to access an account is, in fact, the actual holder of the account. However, websites must still be able to recognize users who can't provide their correct password, as the password might be lost, forgotten, or even stolen. Also the users friend or acquaintance or a stranger can access the social network profile of user to know information about user which he can use to guess the password of a user and get access to his/her social network profile. In this case, users will require to authenticate themselves.Various system use various different kind of secondary authentication.

It's no secret. Measuringthe security and reliability of authentication via secret questions.

This paper was published by S. Schechter, A. B. Brush, and S. Egelman in the year 2009.

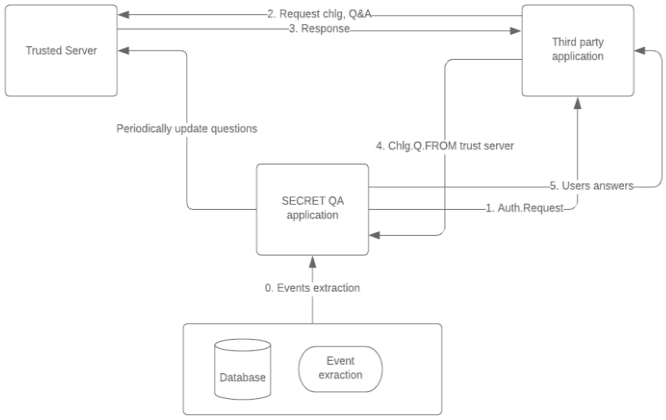
This paper shows that the questions set by user himself is vulnerable to attacks and threats by complete stranger or users acquaintance.

III. PROPOSED SYSTEM

Here we discuss our proposed system which mainly consists of 3 challenges which are as below:

1. The User-Event Extraction Scheme
2. Periodically Updating Questions
3. Request-Challenge Mechanism

The above three challenges are implemented as shown in the architecture block diagram below.



The above Figure Block architecture of System, for a typical user scenario of resetting the account password through answering the secret questions.

A Three-Phase Challenge Response Protocol:

As shown in Fig. 1 (from step 1 – 5), whenever a user needs to identify himself to get access to the application through our trusted servers the system throws out a set of security questions to authenticate his identity and following operations are carried out.The following three operations are carried out.

- Issue(Request)
- Challenge(Users response).
- Authentication(Access).

IV. CONCLUSION

In this paper, we present a Secret-Question based Authentication system, called "Secret-QA", and make use of user's short term memory and smart phone sensors to create a set of questions that update periodically and provides secondary authentication to the system. The question make use of various sensors of the smart phone and develop a set of questions that only a user of the system know answers of also the system updates its questions periodically while maintaining a threshold of 80 percent correctness of the users answers to provide access of the system to the corresponding user.

REFRENCES

[1]. M. Zviran and W. J. Haga, "User authentication by cognitive passwords: An empirical assessment," in Proc. 5th Jerusalem Conf. Inf. Tech., Next Decade Inf. Tech., (Cat. No. 90TH0326-9), 1990, pp. 137–144.

[2]. J. Podd, J. Bunnell, and R. Henderson, "Cost-effective computer security: Cognitive and associative passwords," in Proc., 6th Australian Conf. Comput.-Human Interaction, 1996, pp. 304–305.

[3]. S. Schechter, A. B. Brush, and S. Egelman, "It's no secret. Measuring the security and reliability of authentication via

secret questions," in Proc. 30th IEEE Symp. Security Privacy., 2009, pp. 375–390.

[4]. A. Rabkin, "Personal knowledge questions for fallback authentication: Security questions in the era of facebook," in Proc. 4th Symp. Usable Privacy Security, 2008, pp. 13–23.

[5]. J. C. Read and B. Cassidy, "Designing textual password systems for children," in Proc. 11th Int. Conf. Interaction Des. Children, 2012, pp. 200–203