International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/IJSRCSEIT

Review on Security for Mobile Applications Using Mobile Sensors

Amey Shimpi[1], Sanket Sakore[2], Charudatta Pawar[3], Sejwal Lad[4], Prof. Yogesh Thorat[5]

[1,2,3,4] Student, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegoan Savitribai Phule Pune University, Pune, Maharashtra, India

[5] Professor, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegoan Savitribai Phule Pune University, Pune, Maharashtra, India

ABSTRACT

In todays growing world of technology more and more mobile applications are getting developed day by day and with the increased growth of application the threats for user's accounts present in the applications being hacked by hackers is also increasing at a great rate. The proposed system focuses on increasing the privacy of mobile application when the user forgets the password by asking security questions based on user's daily activity and even at the time of password generation it provides newly introduced advance feature to set new password. Security questions asked by the system to user are based on the inbuilt mobile sensors which trace the user's location and call logs and deals with many other sensors present in the android mobile devices to authenticate the answers given by the user for the questions asked by system.

Keywords : Mobile Sensors, Android Application, Security Questions, Password Generation

I. INTRODUCTION

Every mobile application which are used to provide access for the user to it's personal details like online banking app, Gmail account, yahoo, msn etc. consist of password for login purpose and this passwords are tricky consisting combination of alphanumeric and special symbols to remember such tricky password is very inconvenient job. If the user forgets the password due to some reason or mistype it then he/she can't access their accounts. To get the access of account user must answer some security questions which along with the answer are recorded at the time of user registration.

After a long time, interval it becomes difficult for the individual to remember answer of questions and at the same time in a world of social media it's very easy for hacker or malicious user to guess the answer. To avoid these problems, we propose a system that can overcome all threats from existing system by using smart phone sensors.

The security questions in the proposed system will be asked to the user by the system itself and those security questions will not be the one which are present in the existing system (e.g., "Who is your favourite movie actor?"). The questions will be based on user activity in short time period which will be generated using mobile sensors and answers to such type of questions need not to be memorized by the user and this questions provides a high-level security to the mobile application and after the user succesfully answer all the security question during the new password generation phase an entirely unique password generation scheme can be applied which will be based upon the location co-ordinates as per the user's dream location.

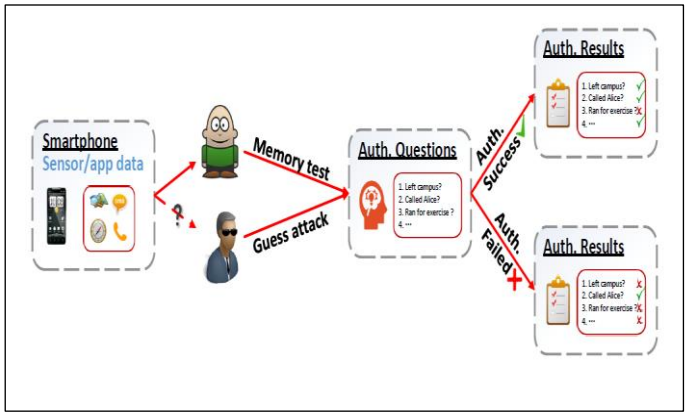

Fig1 : System Architecture of the proposed system

The proposed architecture consists of smartphone which has sensors and the system records the data present in the sensors and ask security questions to the user based upon his/her daily activities. The system authenticates the answer given by the user and if the answers are incorrect it results into authentication failed which will generally happen if any guest user tries to hack the application.

II. RELATED WORK

Peng Zhao, Kaigui Bian, Tong Zhao, Xintong Song, Jung-Min "Jerry" Park, Xiaoming Li, Fan Ye, Wei Yan [1] the related work simply shows the overall idea related to design the security questions likely called as "secret question based authentication system"(Secret-QA) the authors simply designed a prototype on android smartphones and evaluate the security of the secret questions. The secret questions are those based on the smartphone sensors data. Authors evaluated the reliability and security of question mainly of type (multiple choice, yes/no) by involving 88 participants in the survey and found the result that "The Secret-QA is easier to use then the existing system which consist of security questions based on user's long-term data". Basically, this work only consists of analysis how the smartphone sensors will be useful to design the security questions.

M. Oner, J. A. Pulcifer-Stump, P. Seeling, and T. Kaya [2] This paper describes Walk Compass, a system that exploits smartphone sensors to estimate the direction in which a user is walking. This work mainly focus on predicting the falling accidents of the senior citizens though accelerometers and gyroscope can be combined together to detect the fall event but accelerometers are used in different locations and individual find it very difficult and impractical to wear many such sensors on particular location so the author proposed to use mobile smartphone to detect fall event using mobile inbuilt sensors. The initial work is presented on pedometer mobile application component that is used to notify the user's family member about any medical issue through e-mail. The author also developed algorithm which counts the steps and identify type of activity. This work consists of application built with the use of mobile sensors which is like our proposed system which generated security questions using sensors.

R. Reeder and S. Schechter [3] The primary means of authenticating user is password. Though there is always a risk of password getting lost, stolen in technical language to say password being hack, most websites also provide secondary authentication through which user can get the correct password to gain access to account again but if the secondary authentication is user's last resort a false attempt may lead to permanent account loss if secondary authentication mechanism's vulnerability to false attempt is not as strong as that of passwords then such mechanism becomes a weakest link for user friendly environment. The authors highlight results of prior work on secondary authentication mechanisms, emphasizing the larger problem of assembling an arsenal of mechanism that can be customized to fit each user's security and reliability needs.

S. Schechter, A. B. Brush, and S. Egelman [4] Mainly authors performed a case study in this paper by taking four most popular webmail providers- AOL, Google,

Microsoft and Yahoo! into consideration and found that the authentication based on the secret question mainly requires only one question in order to reset an account's password. They perform a user study to measure the reliability and security of the questions by asking some individuals to answer the questions and then asked their acquaintances to guess their answers and found that the acquaintances were able to guess 17% of answers which the participants were unwilling to share and also found that nearly about 20% of participants forgot their answers within six months. And even suggests that according to the survey done in 1996 with the inclusion of participants and their close friends or family members nearly about 33%-39% were able to guess correct answer and 20%-22% participants forgot their answers. Accordingly, the author found that security questions which more likely are said as secret questions don't have any higher level of security.

III. COMPARISON

According to the literature survey the work of mobile sensors and secondary authentication using security questions says that existing system doesn't use any type of mobile sensors for security purpose it only consists of security questions for authentication purpose which consist of answers depend on the long term history and even the hackers can easily guess the answer of such questions using social media or any other techniques and also in the real time user find it very difficult to remember answer of such questions. In our proposed system we are trying to overcome such problem which occurs at the time of authentication. As we are using mobile sensors so user itself find it very safe and easy way to understand the overall mechanism and the proposed system even overcomes the threats or any attack as the questions will the based on the user's daily activity by using the technique of Secret Question based authentication (Secret-QA).

Proposed system also provides a newly introduced feature of password generation by allowing the user to select his/her dream location and with the help of location co-ordinates set the password which is a completely new concept in the field of password generation. So, the comparison between the existing and proposed system clearly defines that we are trying to build such an environment in the field of user's account privacy so that the only person who can smoothly take the advantage of this features will be the user itself without any worry.

IV. CONCLUSION

The proposed system will overcome the drawbacks of the existing system. In this paper we discuss about how the privacy of the mobile application can be taken to the next level by designing the system in such a way that it asks security questions to user by using the mobile sensors present in the smartphones and those questions are system generated and not like the traditional questions present in the existing system. In future proposed system will be very helpful as it may consist the second part after answering the security questions. This project can further extend to set the password based upon the location co-ordinates which will be more efficient for providing security.

V. ACKNOWLEDGEMENT

We would like to thank Dr. D. Y. Patil School of Engineering for providing us with all the required amenities. We would thank our guide Prof. Yogesh Thorat sir for giving us all the help and guidance we needed. We are also grateful to Dr. Pankaj Agarkar, Head of Computer Engineering Department, DYPSOE, Lohegaon, Pune for their indispensable support, suggestions and motivation.

VI. REFERENCES

[1]. Peng Zhao, Kaigui Bian, Tong Zhao, Xintong Song, Jung-Min "Jerry" Park, Xiaoming Li, Fan Ye, Wei Yan, Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions, pp.99, 2016.

[2]. M. Oner, J. A. Pulcifer-Stump, P. Seeling, and T. Kaya, Towards the run and walk activity classification through step detection-an android application, in EMBC. IEEE, 2012, pp. 1980–1983.

[3]. 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.

[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]. H. Kim, J. Tang, and R. Anderson, Social authentication: harder than it looks, in Financial Cryptography and Data Security. Springer, 2012, pp. 1–15.

Cite this article as :

Amey Shimpi, Sanket Sakore, Charudatta Pawar, Sejwal Lad, Prof. Yogesh Thorat, "Review on Security for Mobile Applications Using Mobile Sensors", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 8, pp. 25-28, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT19487