

Secret Questions based Authentication System for Android Smartphone

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

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

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

Guide: Mrs.R.V.Chaudhari
Assistant Professor,
Computer Department
Met blujbal 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 a basic android 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 retrieval 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 actual 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 through 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 guessed 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 lightweight Yes/No questions and MCQ's required less amount of input effort with the same strength as compared by blank-filling questions.