Enhancing Security Of Secret Question By Using Smart phone Sensor

Miss.**Avhad Priyanka**, Miss.**Mali Nikita**, Mr.**Pawar Kiran**, Mr.**Sonaje Nikhil**, Prof.V.A.Hiray

***Abstract*: Many web applications provide secondary authentication methods, i.e. secret questions (or password recovery questions), to reset the account password when a user's login fails. However, the answers to many such secret questions can paper,we present a Secret-Question based Authentication system, called be easily guessed by an acquaintance or exposed to a stranger that has access to public online tools (e.g., online social networks); moreover,a user may forget her/his answers long after creating the secret questions.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. In this Secret QA", that creates a set of secret questions on basic of people's 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.Observe the questions' reliability by asking participants to answer their own questions. To remind modern people of something at a speci**fy **time and location , Smart Location Reminder is a boon . To serve the purpose, implementing an application for Android-based smart phones and tablets which is not only time based but also location based.**

INTRODUCTION

The security of a secret question depends on the validity of a hidden assumption: A users long-term personal history/information is only known by the user himself. However, this assumption does not hold when a users personal information can be acquired by an acquaintance, or by a stranger with access to public user paroless. An acquaintance of a user can easily in farther answers to the users secret questions (e.g., name of pet). Moreover, as stranger cangure out the answers leaked from public user paroles in online social networks or search engine results (e.g., the hospital your youngest child was born in).The reliability of a secret question is its memo ability the required or dificulty of memorizing the correct answer. Without a careful choice of a blankingsecret question, a user may be declined to log in, because he cannot remember the exact answer that he provided, or he may miss pill the input that requires the perfect literally-matching to the correct answer.

OVERVIEW

The User-event Extraction: Scheme Todays 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: (1)the common sensors equipped on the top-ten best-selling smart phones in 2013, (2) the top-ten downloaded Android apps in 2013, and (3) the legacy apps (Call, Contact, SMS, etc.), as shown in Table I. Because these sensors and apps are already built-in for almost all the smart phones, our approach is naturally suitable for smart phone users without introducing any extra hardware costs.Secret-QA client app: 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. As shown in the block diagram (the step 0 in Figure 1), the client app schedules the feature extraction process periodically, and then features will be recorded in the local databases. For example, we adopt lib SVM [15] on Android to detect motion related user events, and we roughly set the minimum duration to 10 minutes For noise removal (details on how to create questions and algorithms for other types of events extraction will be given in Section IV). Note that our extraction of user events are most lazily scheduled using Android Listener [16] to save battery; meanwhile, we will pause the scheduling for some sensors after the screen is locked (e.g., app usage), because no events can happen during screen-lock periods. 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.

PROBLEM DEFINATION

The proposed System overcome the drawbacks of authentication precess in real time. 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 articipants to answer their own questions. Our experimental results reveal that the secret questions related to motion sensors, calendar, app installment, and part of legacy app usage history (e.g., phone calls) have the best memorability for users as well as the highest robustness to attacks.

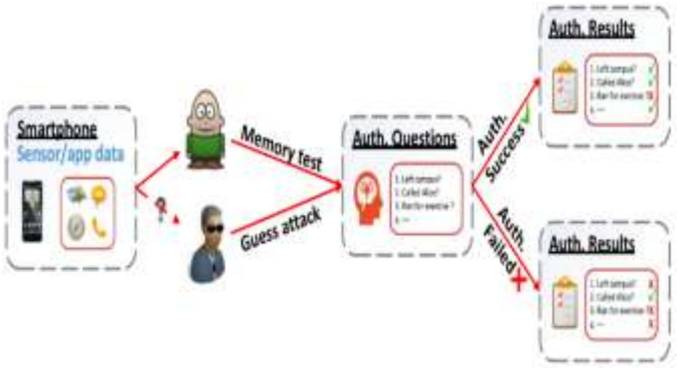
LITERATURE SURVEY

1. When the Password Doesn't Work: Secondary Authentication for Websites: *In this Nearly all websites that maintain user-specific accounts employ passwords to verify that a user attempting to access an account is, in fact, the account holder. However, websites must still be able to identify users who can't provide their correct password, as passwords might be lost, forgotten,or stolen. In this case, users will require a form of secondary authentication to prove that they are who they say they are and regain account access. Websites can use a variety of secondary authentication. The article discusses secondary authentication mechanisms, emphasizing the importance of assembling*

2. User authentication by cognitive passwords: An empirical assessment The concept of cognitive passwords is introduced, and their use as a method to overcome the dilemma of passwords that are either difficult to remember or easily guessed is suggested. Cognitive passwords are based on personal facts, interests, and opinions that are likely to be easily recalled by a user. A brief dialogue between a user and a system, where a user provides a system with exact answers to a rotating set of questions, is suggested to replace the traditional authentication method using a single password. The findings of an empirical investigation focusing on memorability and ease of-guessing of cognitive passwords, are reported.

3. Cost-effective computer security: Recall and guessing rates for conventional, cognitive, and word association passwords were compared using 86 Massey University undergraduates. Respondents completed a questionnaire covering all three password types, returning two weeks later for a recall test. Each respondent also nominated a"significant other" (parent, partner, etc.) who tried to guess the respondent'answers. On average, cognitive items produced the highest recall rates (80%)but the guessing rate was also high (39.5 per). Word associations produced low guessing rates (7 per) but response words were poorly recalled (39 per). Nevertheless both cognitive items and word associations showed sufficient.

WORKING OF SECURITY QA



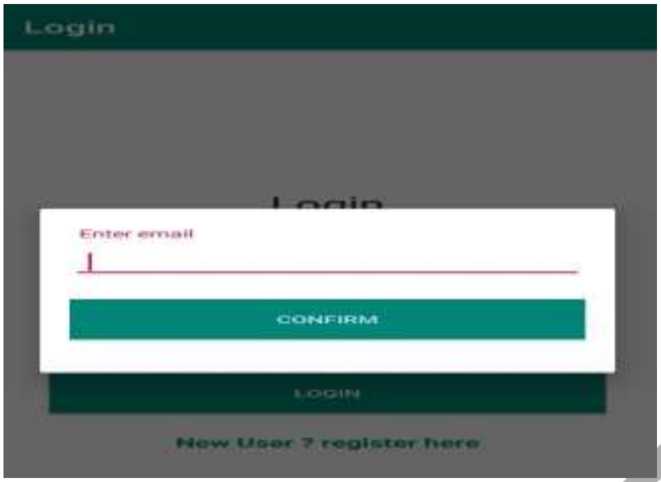
:

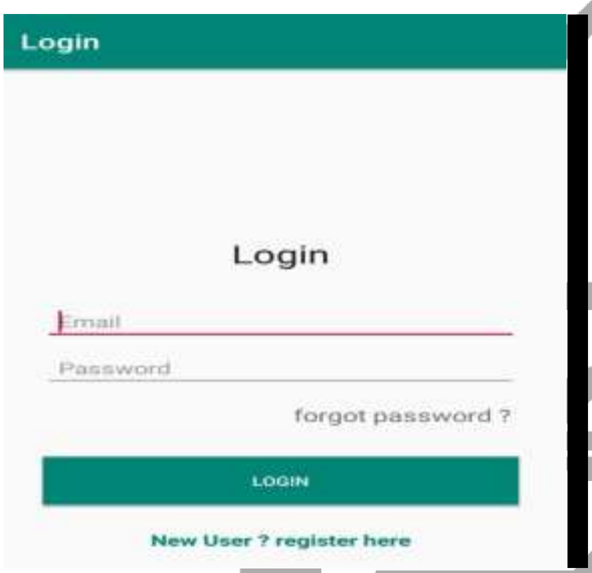
a.1:-Nave bayes based Recommendation Algorithm

The data set for which we have taken the data as a training set and tried applying the algorithms on it by taking the data of past as a test set and then view the output. This obtained output is compared with the actual output. Crop with maximum points can be recommended to the farmer. The market trend of the crops is saved in the database. While recommending more than one of the crops, the factor determined will be the year factor that will be followed by market factor and the ratio factor. For recommending the crop to the user, we are using the nave bayes algorithm. A naive Bayes classier is asimple probabilistic classifier based on applying Bayes39; theorem with strong (naive) independence assumptions. Depending on the precise nature of the probability model, naive Bayes classifiers can be trained very efficiently in a supervised learning setting. An advantage of the naive Bayes classifier is that it only requires a small amount of training data to estimate the parameters

(means and variances of the variables) necessary for classification.

I. RESULTS





ADVANTAGE

- Id Will be more secure
- Only the authorized user can get access to the File
- Centralized Management
- Secure Authentication
- No one can guess easily when forgetting password

DISADVANTAGE

- Someone not know about the Usage
- People will need to be more aware about the Data usage

CONCULSION

Hence 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 reect 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. In our experiment, 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 history/information.

REFERENCES

[1] R. Reeder and S. Schechter, When the password doesnt work: Secondary authentication for websites, S P., IEEE, vol. 9, no. 2, pp. 4349, 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. 137144.

[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. 304305
.

[4] S. Schechter, A. B. Brush, and S. Egelman, Its no secret. Measuring the security and reliability of authentication via secret questions, in S P.,IEEE. IEEE, 2009, pp. 375390.

[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. 18.

[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. 1323.

[8]. J. C. Read and B. Cassidy, Designing textual password systems for children, in IDC., ser. IDC 12. New York, NY, USA: ACM, 2012, pp200203.SIER