ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

Secret QA System Using Legacy App Usage History

Archana Chindhu Bhaware[1], Prof.Harish Barapatre[2].

Department of Computer Engineering, YTIET, Karjat, Maharashtra, India[1,2]

ABSTRACT: At present with increasing popularity of online shopping Debit or Credit card fraud. Personal information security is major concerns for customers, merchants and banks specifically in the case of Card Not Present. 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. 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. We also provide a secure system for barcode based visible light communication for online payment system using image stenography methodology. We present a Secret-Question based Authentication system, called "Secret- QA"that creates a set of secret questions on the basis 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 we observe the questions reliability by asking participants to answer their own questions.

KEYWORDS*:* Secret Question,Autentication

I. INTRODUCTION

SECRET QA SYSTEM

Security QA system provided by password-based login is insufficient for customers, especially in the financial sector. An administrator can set up security questions. After providing the correct login name and password, a user (Smart phone) must answer selected question(s) before proceeding to application pages.

Now-a-days,use of Smartphone apps has been increased. There are some important transaction related apps requires more authentication so that Secondary Authentication Feature is essential for such apps for security concern. Most of the apps need to make registration, which includes set of secret questions based on only personal information, where user has to choose some question and provide answers to selected questions.Those questions are next used for recovery of password.Where correctness of answers are checked for authentication purpose, and only if right user is using it and giving correct answers then only he or she can able to reset or recover password.

Through public user profiles, user's personal information can be easily guessable by friends or closers, strangers. These public profiles can be obtained from online social media like face book, twitter or from results of different search engines.

This results in loss of reliability. For reliability, user has to memorize correct answers for security questions. User can face difficulty to remember correct answer for each question. So questions are asked based on user's recent Smartphone usage. SMS,Location,Call log questions and Calendar event questions are included. Where user only needs to remember short term data related to Smartphone usage like 'To whom user recently called','To whom he sent SMS',etc. Some questions are based on analysis of log data. These questions are based on duration of calling and frequently made calls.In this paper presenting "Secret QA System Using Legacy App Usage History", has benefits like:

- Does not need to remember all history about Smartphone usage.
- Set of questions provided through combination of personal and log based questions (SMS, Call, Location, and Calendar).

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

- Security is based on 70% correct answer given by user.

II. LITERATURE SURVEY

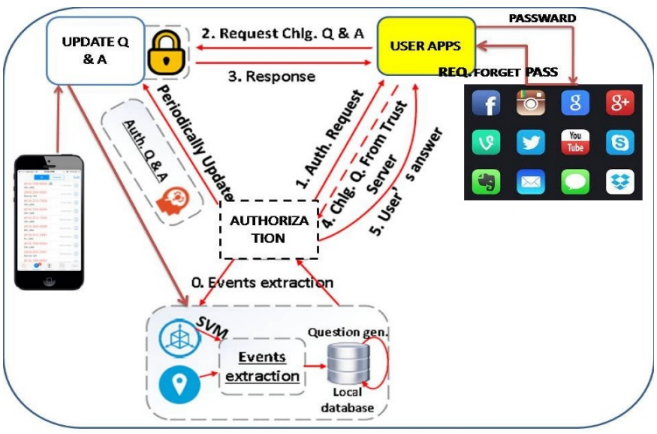
1.R. Reeder and S. Schechter, When the password doesn't work: Secondary authentication for websites ' S & P., IEEE, vol. 9, no. 2, pp. 4349, March 2011. Nearly all websites that maintain user-special accounts employ passwords to verify that a user attempting to access an account is, in fact, the account 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 mechanisms.

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 IEEE, 1990, pp. 137144. This project introduces the concept of cognitive passwords and suggests their use as a method to overcome the dilemma of passwords that are either difficult to remember or that can easily be guessed. 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 mending pending of an empirical investigation, focusing on memorability and ease-of-guessing of cognitive passwords, are reported. These endings demonstrate that cognitive passwords were found to be easier to recall than conventional passwords, while being difficult for others to guess, even others who are close to the users.

III. PROBLEM DEFINATION

To developed 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 participants to answer their own questions. This work is to study whether using Smartphone sensor/ app data is helpful for secret-question based secondary authentication. People like students have the necessary experience on setting and answering secret questions and they use Smartphone's and online tools every day.

The methodology approach used for this application is the top down approach is essentially the breaking down of a system to gain insight into its compositional subsystems. In a top-down approach an overview of the system is specified but not detailing any first level. In early days all are uses android phones, it transfers data easily and faster. It is very easy to use an application anywhere and anytime. There are some issues:



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

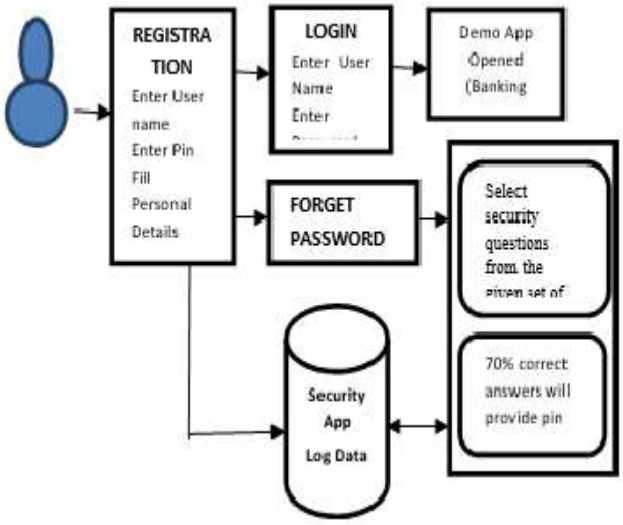
1. Authentication
2. Security of confidential data

They emphasized that frequently-changing secret questions will be difficult for attackers to guess the answers. However, this research is based on the data related to a user's Internet activities, while our work leverages the mobile phone sensor and app data that can record a user's physical world activities, for creating secret questions. For better reliability, one may choose other types of secret questions rather than blank-filling questions to avoid the difficulty in recalling and inputting the perfect literally-matching answer.

IV. PROPOSED SYSTEM

The "reliability" of a secret question is its memorability the required effort or difficulty of memorizing the correct answer. Without a careful choice of a blank filling secret question, a user may be declined to log in, because he cannot remember the exact answer that he provided, or he may misspell the input that requires the perfect literally-matching to the correct answer. We design a user authentication system with a set of secret questions created based on the data of users' short-term smart phone usage. We evaluated the reliability and security of the three types of secret questions (blank-filling, true/false, and multiple-choice) with a comprehensive experiment involving 88 participants. The experimental results show that the combination of multiple lightweight true-false and multiple choice questions required less input effort with the same strength provided by blank-filling questions.

Block Diagram of System-



SYSTEM ARCHITECTURE:

The Secret-QA system consists of two major components, namely the user-event extraction scheme and the challenge response protocol, which is shown in Figure and will be elaborated next.

1.The User-event Extraction Scheme

Today's Smartphone's are typically equipped with a plethora of sensors and apps which can capture various events related to a user's daily activities, e.g., the accelerometer can record the user's sports/motion status without consuming excessive battery.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

2.A Three-phase Challenge Response Protocol

The service prescribes three phases for authentication

Issue-The user issues an authentication request to the service provider, then the OSN website asks our trusted server for one or more encrypted secret questions and its answers, the questions are finally transferred to the user displaying on the Smartphone's (in Above Figure). The information at this phase must be sent over a secure channel against the malicious eavesdroppers.

Challenge:The user provides answers to the challenge questions according to his/her short term memory, and then sends it back to the OSN website (in Above Figure).

Authentication:The authentication is successful if the user's response conforms to the correct answers; otherwise, a potential attack is detected. If the times of authentication failure exceeds the threshold, our trusted server would deny to provide service for this particular user, as the in the last step The interactions with server are also necessary to improve the resilience to some obvious attack vectors in local operation mode. For instance, if a user's mobile phone is Stolen / lost (or the user has been followed by a stranger for days), the user can disable EvenLog functionality (or remote lock/swipe out the phone) to eliminate the danger of potential adversary who records the users recent activities with the help of server.

V. METHODOLOGY

Types of secret questions:

A. True/false Questions-

Location (GPS) related questions.The example question related to GPS is No. 1 "Did you leave campus yesterday?. The GPS sensor captures the location information of the participants, so that we could easily learn whether participants left campus far away enough with GPS coordinates recorded. Since that the coarse-grained GPS data has a typical mean error of 500 meters as described in Android API reference, and thus we determine a participant leaves the campus when the GPS location is 500 meters out of the campus area.

B. Multiple-choice and Blank-filling Questions-

We create "W" questions in the form of multiple-choice and blank-filling by simply extending the true/false questions on legacy and third-party apps. For example, true/false questions can be easily extended to be a "W" question: "who did you call/text?" (Incoming and outgoing calls, or a frequency-based "W" question: "Which app did you use most frequently?". Answers to multiple-choice questions. For each multiple choice question, there are four options (only one correct option). The correct option is randomly picked with an equal probability of being any options.

SVM Based Information Extraction scheme:

Information Extraction is a token classification task rather than a Text Classification task. With Information Extraction we are working with texts but the basic units that we are looking for to classify are tokens in the text rather than the entire text. With Text Classification we are seeking to identify whether an entire text is a member of particular category, while in Information Extraction the categories are start and end, and the objects we seek to assign to these categories are the individual tokens. Additional information about the token are encoded to enable SVM learning algorithm to generalize. Several features of the token as well as relational information about the surrounding tokens can be encoded. SVM Based Information Extraction in this project is employing GATE (General Architecture for Texts Engineering) toolkit. Machine learning process in GATE is based on SVM Light Wrapper.

Two steps of this Information Extraction are training and extraction. Training process is to build a classifier for certain tag. This process is started with annotating sample corpus with targeted slots. In order to build the SVM model, we require start and end annotations for each class of annotation. SVM parameters are selected to build the model. Once the model becomes available, SVM classifier classifies the unseen documents which creates the annotation for start and tag over the text on training process for SVM, first corpus is stored in a GATE format and annotated in accordance with the token type (e.g. commodity) and this document is used as an input to build SVM model (which is needed <commodity> as start tag and </commodity> as end tag on the object text/token in question). SVM models are

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

generated and stored in an external file/record for later use. In this project to build the features vector of tokens, several NLP features are used. First, Case/Orthography, which is the use of uppercase and lowercase letters by the token. Second, Types of tokens i.e. words, numbers, symbols, or punctuation. Third, Entity, the output module of named entity recognition standards owned by GATE. The window size is the number of tokens before and after the target token. It is also used as an input for SVM. In SVM-GATE system, two SVM classifiers for each type of entity, one classifier for the start and another one for the end word, are trained. One-word entities are regarded as both starts and end. In contrast, trained four SVM classifiers for
each named entity type besides the two SVMs for start and end, also one for middle words, and one for single word entities. They also trained an extra SVM classifier to recognize words that do not belong to any named entity. Trained an SVM classifier for every possible transition of tags so that may lead to a large number of SVM classifiers. As our SVM classifiers only identify the start or end word for every target class, some post processing is needed to combine these into a single tag. To extract information from a new document, the system requires the SVM model produced in the learning process. SVM classifiers then will annotate text with the initial tag and the end tag that match existing models. In the next stage, the start and the end tags are combined in an appropriate token.

For example, given this annotated text:

There will a talk by <speaker>Laura Petitto</speaker> tomorrow morning. On learning phase, each word will be used as an example of following classes:

not start tag = {“there”, “will”, “a”, “talk”, “by”, “Petitto”, “tomorrow”, “morning”}

not end tag = {“there”, “will”, “a”, “talk”, “by”, “Laura”, “tomorrow”, “morning”} start tag = {“Laura”}
end tag = {“Petitto”} Given this new text,
To remind you that Bill Gates will arrive at noon.

On extraction phase, SVM Classifier will classify the new text as follow:

not start tag = {“To”, “remind”, “you”, “that”, “Gates”, “will”, “arrive”", “at”, “noon”}

not end tag = {“To”, “remind”, “you”, “that”, “Bill”, “will”, “arrive”", “at”, “noon”} start tag = {“Bill”}
end tag = {“Gates”}

After post processing, start tag and end tag will be combined into a single tag
<speaker>Bill Gates</speaker>.

VI. IMPLEMENTATION & RESULT ANALYSIS

when we have logged that time it shows the incorrect password so how to login my application or how to recover my password. We don’t want to create a new password but we recover my original password. So I was click on forget password so the system has generated the 3 question regarding our Smartphone and the main thing is that the smart answer know only the smart user. If smart users are unable to give the answer of the question or less than 73.00% than it will consider as attacker. These apps was tested on 3 different company smart phone and every smart phone we have created 20 to 24 users data. Final result analysis was shows on the graph.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

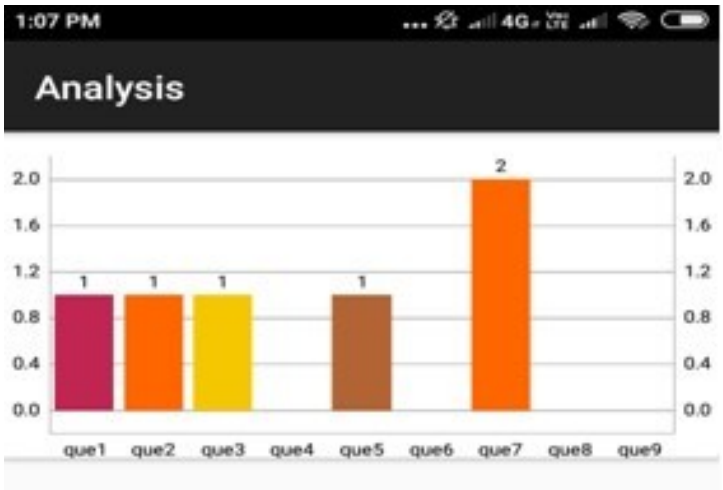


Figure 1 : analysis graph

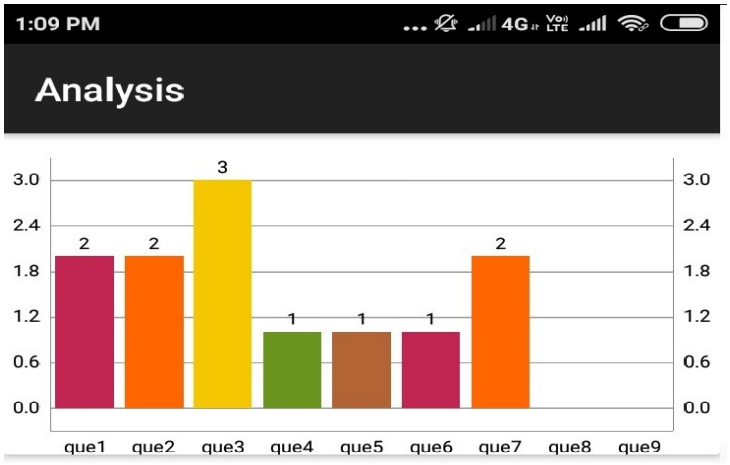


Figure 2: analysis graph

Total number of question and easily analysis the how many times we have give the correct answer of every question also which question we have not provide the correct answer. The main basic thing of this project we have provided the best security to every app from attackers and safely login. The finally we have analyze the all question that means which question got the correct answer and which question got the wrong answer so on that basis we have improve our security and easily secure the data from outsider. The main outcomes from this project is the secret questions related to motion sensors, calendar, app instalment, 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 user's long-term history/information. In this system, our research provides a gridline that shows. Which sensors/app data and which type of question are suitable for devising secret question. This implies improved security for such secret questions

.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

VII. APPLICATION

- Online social network
- Online banking
- Online shopping
- Web application
- It is easier to memorize the SMS record in a long period of time for emerging adults, but it is better to memorize the call record in a short term.
- It is easier to answer Yes/No questions rather than frequency based questions.
- College students' offline communication behaviors via phones are different from their online behaviors over the OSNs. Thus, online tools can be misleading when answering the secret questions related to offline call and SMS activities.

VIII. CONCLUSION

We Proposed a Secret QA System Using Legacy App Usage History, called "My secret QA", and lead a client concentrate to see how much the individual information gathered by cell phone sensors and applications can help enhance the security of mystery inquiries without damaging the clients' protection We make an arrangement of inquiries in light of the information identified with sensors and applications, which mirror the clients' transient exercises and cell phone utilization. We measure the dependability of these inquiries by requesting that members answer this inquiry, and in addition propelling the associate/more peculiar speculating assaults with and without help of online apparatuses, and we are thinking about setting up a probabilistic model in light of a substantial size of client information to describe the security of the mystery questions.

REFERENCES

[1]Peng Zhao, Kaigui Bian "Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions", IEEE Transactions on Mobile Computing (Volume:PP , Issue: 99),24 March 2016
[2]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.
[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. 304–305.
[4]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. 1–8.
[5]D. A. Mike Just, "Personal choice and challenge questions: A security and usability assessment," in Proc. 5th Symp. Usable Privacy Security, p. 8. ACM, 2009.
[6]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.
[7]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, 2013, pp. 137–144.
[8]H. Kim, J. Tang, and R. Anderson, "Social authentication: harder than it looks, in Financial Cryptography and Data Security". Springer, 2012, pp. 1–15.
[9]N. Roy, H. Wang, and R. R. Choudhury, "I am a smartphone and I can tell my user's walking direction", in Proc. ACM MobiSys, 2014, pp.329–342.