ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

A Survey on Password Recovery System for Android Mobile Phones

Komal Jagtap[1], Poonam Sonawane[2], Harshada Nikam[3], Tejashree Jagtap[4], Dhanashri Jagtap[5]

Prof. Jyoti Deshmukh[6]

Department of Computer Engineering, JSPM BSIOTR Wagholi, Pune, India[1,2,3,4,5,6]

ABSTRACT: At present with increasing popularity of online shopping Debit or Credit card fraud. Personal information security are 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: security, smart phone, secret question.

I. INTRODUCTION

Secret questions (password recovery questions) have been widely used by many web applications as thesecondary authentication method for resetting the account password when the primary credential is lost. When creatingan online account, a user may be required to choose a secret question from a pre-determined list provided by theserver, and set answers accordingly. The user can reset his account password by providing the correct answers to thesecret questions later. For the ease of setting and memorizing the answers, most secret questions are blank-fillings (a.k.a. fill-in-the-blank, or short-answer questions), and are created based on the longterm knowledge of a user's personal history that may not change over months/years (e.g., "What's the model of your first car?"). However, existing research has revealed that such blank-filling questions created upon the user's long term history may lead to poor security and reliability.In this paper, we present a Secret-Question based Authentication system, called "Secret-QA", taking advantage of thedata of smart phone sensors and apps without violating the user privacy. Meanwhile, we develop a prototype of Secret-QA, and conduct an experimental user study involving 88 volunteers to evaluate the reliability and security of the setof secret question created in the system. Specifically,

- In this system if user forget his/her password at that time user can choose secret question or Visual cryptography technique.
- In this system design a user authentication system with a set of secret questions created based on the data of users'short-term smart phone usage.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

- The system 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.

- The system evaluate the usability of the system, and find that the Secret-QA system is easier to use than thoseexisting authentication system with secret questions based on users' long-term historic data.

II. LITERATURE SURVEY

In this paperAt present with increasing popularity of online shopping Debit or Credit card fraud. Personal information security are 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. The present a Secret-Question based Authentication system, called "Secret-QA" that creates a set of secret questions on basis of people's Smartphone usage. The develop a prototype on Android smart phones. The design a user authentication system where user register into system by providing name, mobile number, email id. User login with user name and secret location with secret keyword. If user forget the secret location or secret keyword then user will answer set of secret questions created based on the data of user's daily activity and short-term Smartphone usage. Feature selection will be applied to select question type by data collected from mobile sensors. The questions can be true/false type secret questions. These question are easy to answer and no need to remember because those are on based on user personal life and events. Due to this application security will be enhance because only user knew the events and things he/she did recently. [1]

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 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 smartphones has granted us new opportunities to observe and understand how the personal data collected by smartphone sensors and apps can help create personalized secret questions without violating the users' privacy concerns. In this paper, The present a Secret-Question based Authentication system, called "Secret-QA", that creates a set of secret questions on basic of people's smartphone usage. [3]

The propose to strengthen user-selected passwords against statistical-guessing attacks by allowing users of Internet-scale systems to choose any password they want also long as it's not already too popular with other users. The create an oracle to identify undesirably popular passwords using an existing data structure known as a count-min sketch, which the populate with existing users' passwords and update with each new user password. Unlike most applications of probabilistic datastructures, which seek to achieve only maximum acceptable rate false-positives, the set a minimum acceptable false-positive rate to confound attackers who might query the oracle or even obtain a copy of it.[7]

III. PROBLEM DEFINATION

To developed a prototype on Android smart phones, and evaluate. In this system used Visual Cryptography (VC) for providing a facility for critical and confidential data user can choose secret question or VC for password recovery. 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

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. We evaluate the usability of the system, and find that the Secret-QA system is easier to use than those existing authentication system with secret questions based on users' long-term historic data.

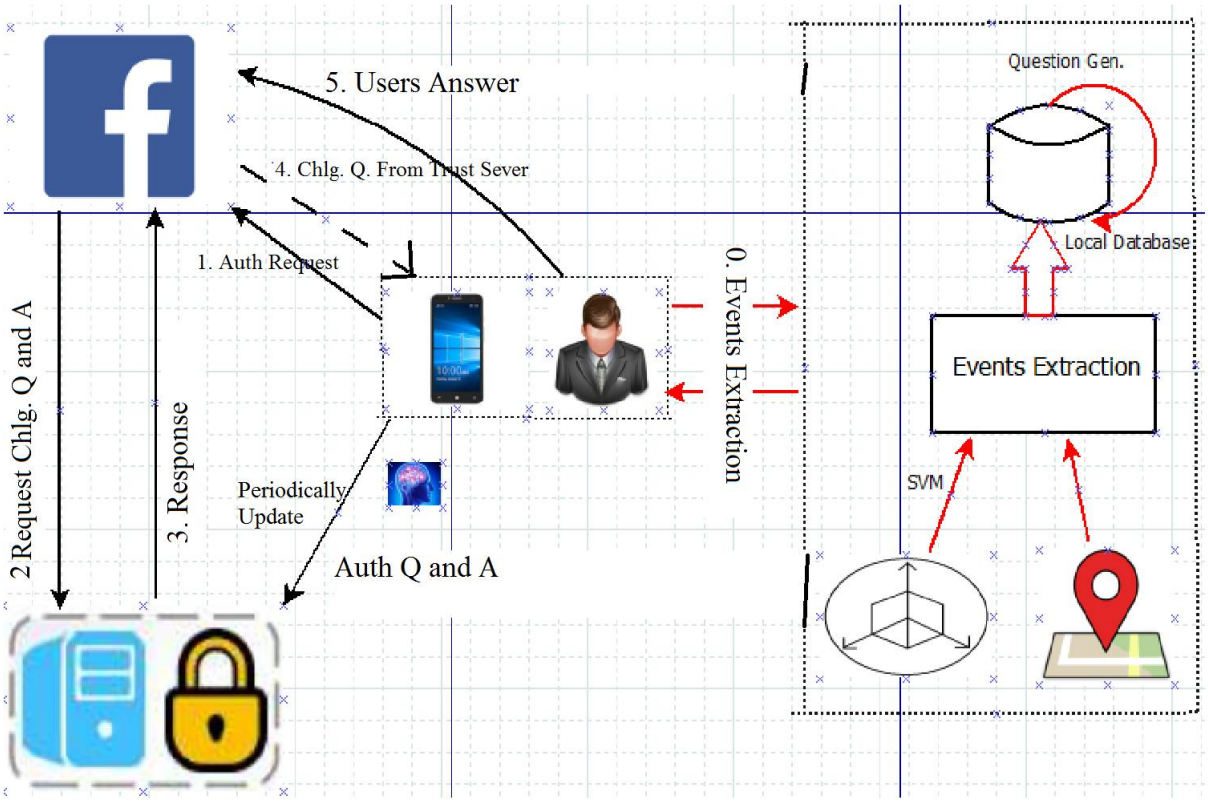

Fig. System Architecture

V. CONCLUSION

In this paper, We Proposed a Secret-Question based Authentication framework, called "Mystery 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 these inquiry, and in addition propelling the associate/more peculiar speculating assaults with and without help

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

of on-line apparatuses, and we are thinking about setting up a probabilistic modelin light of a substantial size of client information to describe the securityof the mystery questions. In our test, the mystery questions identified withmovement sensors, date-book, application portion, and part of inheritanceapplications (call) have the best execution as far as memo ability and theassault exibility, which beat the ordinary mystery question based methodologies that are made in light of a client's long haul history/data.

REFERENCES

[1] 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.
[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. 137–144.
[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] Stuart Schechter, Cormac Herley "Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks"