International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 11 | Nov 2018 www.irjet.net p-ISSN: 2395-0072

Smartphone Sensor Based Security Questions and Location

Ms. Ghodekar P.V [1], Ms. Mogal B. S[2], Ms. Kasar S.R[3], Ms. Deshmukh S. R[4], Prof. Mr. Thosar D.S[5]

[1,2,3,4]B.E Student, computer engineering, SVIT Nashik.
[5]Professor, Dept. of Computer Engineering, SVIT Nashik, Maharashtra, India

---

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 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 paper, we present a *Secret-Question based Authentication* system, called "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, we observe the questions' reliability by asking participants to answer their own questions. To remind modern people of something at a specific 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.

***Key Words*: Sensor fusion, Authentication, Insurance, Invasive software (e.g., viruses, worms, Trojan horses), Physical security, Unauthorized access, Location based reminder, GPS, Mobile Application**

I. INTRODUCTION

SECRET questions (a.k.a password recovery questions) have been widely used by many web applications as the secondary authentication method for resetting the account password when the primary credential is lost [1]. When creating an online account, a user may be required to choose a secret question from a pre-determined list provided by the server, and set answers accordingly. [2], The user can reset his account password by providing the correct answers to the secret questions later. [3], 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)[4], and are created based on the long term 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 [5], [6]. The "security" of a secret question depends on the validity of a hidden assumption: A user's long-term personal history /information is only known by the user himself. However, this assumption does not hold when a user's personal information can be acquired by an acquaintance or by a stranger with access to public user profiles. An acquaintance of a user can easily infer the answers to the user's secret questions (e.g., "name of pet") [4]. Moreover, a stranger can figure out the answers leaked from public user profiles in online social networks or search engine results (e.g., "the hospital your youngest child was born in") [7]. 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 [8]. The recent prevalence of Smartphone 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 feasible to use the knowledge of one's short term personal history (typically within one month) for creating his secret question?

- Intuitively, the short-term personal history is less likely to be exposed to a stranger or acquaintance, because the rapid variations of an event that a person has experienced within a short term will increase the resilience to guess attacks [9], [10]. This implies improved security for such secret questions.
- Moreover, research findings in psychology show that one can easily memorize the details of his short-term activity, if this activity occurs multiple times during a short-term (e.g., calling a friend many times), and/ or this activity heavily involves his time and effort in a short time period (e.g., running exercise) [11].

In this paper, we present a Secret-Question based Authentication system, called "Secret-QA", taking advantage of the data of Smartphone 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 set of secret question created in the system. Specifically,

- We design a user authentication system with a set of secret questions created based on the data of users' short-term Smartphone 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

The rest of this paper is organized as follows: we provide background knowledge in Section 2. In Sections 3, we give an overview of the system design. We present our approach of creating secret questions in Section 4. In Sections 5 and 6, we evaluate the system performance over all created secret questions. We conclude the paper in Section 7.

2. OBJECTIVE

1. To make question papers with varied questions and which meet learning objectives of the course.

2. To generate the question paper from teacher entered specification within few seconds.

3. To cover all aspects of the course objectives and avoid duplication of questions in the subsequent exams.

3. LITERATURE SURVEY

The blank-filling secret questions are dominant as the mainstream authentication solution, especially in web and email authentication systems [1], despite the criticism on its security and reliability. Guessing Attacks by Acquaintance and Stranger. The security of secret questions for authentication was studied by Zviran and Haga in 1990 [2], which indicated that the answers of 33 percent questions can be guessed by the "significant others" who were mainly participants' spouses (77 percent) and close friends (17 percent). Another similar study was conducted by Podd et al, which revealed a higher rate of successful guessing (39.5 percent) [3].

A recent study showed that even an open question written by the user himself was still vulnerable to the guessing attacks launched by his acquaintance [4]. On the other hand, strangers can be more sophisticated than ever to launch the guessing attacks, as they can access the user's personal history through online social networks (OSN) or other public online tools. Therefore, the statistical guessing has become an effective way to compromise a few personal "secret" questions [5] (e.g., "Where were you born?", "What is the name of your high school?"). Poor reliability of secret questions in Real World. Regarding the reliability, a secret question should be memory-wise effortless for users [6]. However, today's mainstream secret question methods fail to meet this requirement.

A recent study revealed that nearly 20 percent users of four famous webmail providers forgot their answers within six months [4]. Moreover, dominant blank-filling secret questions with case sensitive answers require the perfect literally matching to the set answer, which also contributes to its poor reliability. Recent Proposals of User Authentication Systems. To reduce the vulnerability to guessing attacks, Babic et al tried using short-term information such as a user's dynamic Internet activities for creating his secret questions, namely network activities (e.g., browsing history), physical events (e.g., planned meetings, calendar items), and conceptual opinions (e.g., opinions derived from browsing, emails) [12]. 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. For example, the login to an online social network requires a user to recognize one of his friends in a photo [13].

However, it is feasible that a user fails to recognize if he is not familiar to that particular friend chosen by the authentication server. Such existing proposals serve as a good start of using one's short-term activities to create secret questions as well as trying other question types. Since the Smartphone has become one's most inseparable device of recording his life, this paper presents a user authentication system Secret-QA to study on how one's short term history—almost all types of one's activities sensible to the Smartphone—can benefit the security and reliability of secret questions.

Meanwhile, we evaluate the attack robustness of using a combination of many lightweight questions (true/false, multiple-choice) instead of using the blank-fillings, in order to strike a balanced tradeoff between security(and/or reliability) and usability.

4. Architecture Diagram

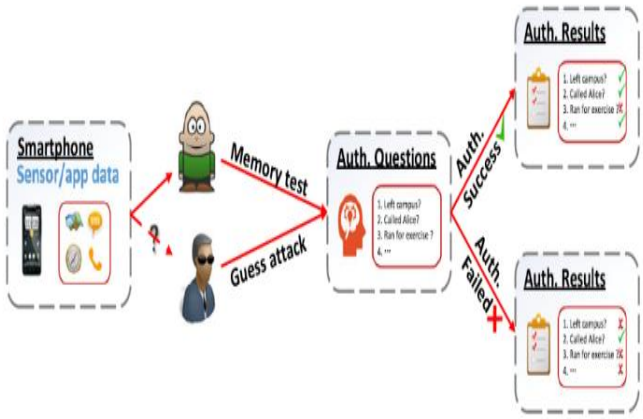

Fig. 1. System architecture of Secret-QA, for a typical user scenario of resetting the account password through answering the secret questions.

Secret-QA Client App. Given the designated sensors and apps for building the authentication system, we develop a Secret-QA client app called "EventLog" to extract the features for question generation. As shown in the block diagram (the step 0 in Fig. 1), the client app schedules the feature extraction process periodically, and then features will be recorded in the local databases. For example, we adopt libSVM [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 4). 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. As shown in block diagram of Fig. 1, when authentication is needed, users' phone can generate questions with local sanitized data and send the answers/results (e.g., how many questions they answered correctly) to auditors via HTTPS channels.

A Three-Phase Challenge Response Protocol

As shown in Fig. 1 (from step 1 – 5), a service provider needs to authenticate the user's identity (typically for resetting the account password) through our trusted server. The service prescribes three phases for authentication.

- Issue: the user issues an authentication request to the service provider (e.g., an OSN website, the step 1 in Fig. 1), 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 smart phones (the step 2 – 3 in Fig. 1). The information at this phase must be sent over a secure channel [15] against the malicious eavesdroppers.
- Challenge: the user provides answers to the challenge questions according to his/her short term memory, then sends it back to the OSN website (the step 4 in Fig. 1).
- 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 in Fig. 1.

Note that 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 Even Log 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.

Threat Models

Former studies including [2], [3], [4] focused on attacks launched by users' significant others or acquaintances, but they ignored malicious guessing attacks from strangers. Moreover, sophisticated attackers could take advantage of online tools to increase their guess rate [5]. Thus, we consider threat models of the two above crossed factors (acquaintance versus stranger; with versus without online tools or external help): (1) acquaintance attacks using online tools, (2) acquaintance attacks without external help, (3) stranger attacks using online tools, (4) stranger attacks without external help.

5. CONCLUSION

In this paper, 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 Smartphone 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 reflect the users' short-term activities and Smartphone 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 question 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 user's long-term history/information.

6. REFERENCES

[1] R. Reeder and S. Schechter, "When the password doesn't work: Secondary authentication for websites," IEEE Security Privacy., vol. 9, no. 2, pp. 43–49, Mar. 2011.

[2] M. Zviran and W. J. Haga, "User authentication by cognitive passwords: An empirical assessment," in Proc. 5th Jerusalem Conf. Inf. Tech., Next Decade Inf. Tech., (Cat. No. 90TH0326-9), 1990, pp. 137–144.

[3] J. Podd, J. Bunnell, and R. Henderson, "Cost-effective computer security: Cognitive and associative passwords," in Proc., 6th Australian Conf. Comput.-Human Interaction, 1996, pp. 304–305.

[4] S. Schechter, A. B. Brush, and S. Egelman, "It's no secret. Measuring the security and reliability of authentication via secret questions," in Proc. 30th IEEE Symp. Security Privacy., 2009, pp. 375–390.

[5] S. Schechter, C. Herley, and M. Mitzenmacher, "Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks," in Proc. 5th USENIX Conf. Hot Topics Security, 2010, pp. 1–8.

[6] 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.

[7] A. Rabkin, "Personal knowledge questions for fallback authentication: Security questions in the era of facebook," in Proc. 4th Symp. Usable Privacy Security, 2008, pp. 13–23.

[8] J. C. Read and B. Cassidy, "Designing textual password systems for children," in Proc. 11th Int. Conf. Interaction Des. Children, 2012, pp. 200–203.

[9] H. Ebbinghaus, Memory: A Contribution to Experimental Psychology. New York, NY, USA: Teachers college, Columbia University, 1913, no. 3.

[10] F. I. Craik and R. S. Lockhart, "Levels of processing: A framework for memory research," J. Verbal Learning Verbal Behavior, vol. 11, no. 6, pp. 671–684, 1972.

[11] T. M. Wolf and J. C. Jahnke, "Effects of intraserial repetition on short-term recognition and recall," J. Exp. Psychology, vol. 77, no. 4, p. 572, 1968.

[12] A. Babic, H. Xiong, D. Yao, and L. Iftode, "Building robust authentication systems with activity-based personal questions," in Proc. SafeConfig. 2009, pp. 19–24.

[13] H. Kim, J. Tang, and R. Anderson, "Social authentication: Harder than it looks," in Proc. 16th Int. Conf. Financial Cryptography Data Security, 2012, pp. 1–15.

[14] S. Hemminki, P. Nurmi, and S. Tarkoma, "Accelerometer-based transportation mode detection on smartphones," in Proc. 11th ACM Conf. Embedded Networked Sens. Syst., 2013, pp. 13:1–13:14. [Online]. Available: http://doi.acm.org/10.1145/2517351.2517367.

[15] (2015). libsvm on android, GitHub [Online]. Available: https:// github.com/cnbuff410/Libsvm-androidjni.