AUTOBIOGRAPHICAL FALLBACK AUTHENTICATION USING SMARTPHONES

Thasni Ebrahim[1], George T Vadakkumcheril[2]

[1]M.Tech Student Computer Science and Engineering
[2]Asst. Professor, Department of Computer Science and Engineering, Indira Gandhi Institute of Engineering Nellikuzhi, Kerala, India

---***---

Abstract - *Various forms of challenge questions are often used as a form of fallback authentication mechanism (a.k.a. backup authentication) to facilitate resetting of passwords or as an extra layer of security if service providers are suspicious of malicious activities. This approach is commonly known as knowledge-based authentication (KBA) scheme. Current KBA schemes can be divided into two categories, namely, static KBA and dynamic KBA. In static KBA, a user usually selects a number of predefined personal questions at the time of account creation. However, the answers to such secret questions can be easily guessed by a stranger who has access to public online tools. Moreover, a user may forget his answers long after creating the secret questions. The widespread presence of smartphones has granted new opportunities to use smartphones to form customized secret questions without violating the user's privacy and security concerns. In this paper present a Secret-Question based Authentication system, called "Autobiographical Fallback Authentication Using Smartphones" that creates a set of secret questions on basic of people's smartphone usage. I developed a prototype on Android smartphones, that collects events from the smartphone itself and authentication provided by asking participants to answer their own questions. The questions related to calendar, app usage, and part of legacy app usage history (e.g., phone calls, SMS) have the best memorability for users as well as the highest robustness to attacks.*

***KeyWords*: Authentication, Password Recovery, Security Questions Autobiographical Authentication, Dynamic Knowledge**

1. INTRODUCTION

Various forms of challenge questions are often used as a form of fallback authentication Mechanism (a.k.a. backup authentication) to facilitate resetting of passwords or as an extra layer of security if service providers are suspicious of malicious activities. This approach is more commonly known as knowledge-based authentication (KBA) scheme. Current KBA schemes can be divided into two categories, namely, static KBA and dynamic KBA. In static KBA, a user usually selects a number of predefined personal questions at the time of registration/account creation .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 long term knowledge of a user's personal history that may not change over months/years such as "What is the name of your first pet?" or "What is the name of the hospital where you born?". Existing research has revealed that such Secret questions created upon the user's long term history may lead to poor security and reliability.

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 once a user's personal information can be acquired by a stranger with access to public user profiles. The "reliability" of a secret question is its memorability—the needed effort for memorizing the proper answer. Without a careful alternative of a blank-filling secret question, a user may be declined to log in, because he cannot remember the exact answer that he provided. Thus, the use of pre-agreed personal challenge questions has been considered to be a weak form of authentication due to poor security and reliability.

To address the limitations of static KBA schemes, recently, dynamic KBA schemes are being investigated where smartphone based autobiographical authentication mechanisms have been explored thus the challenge questions are not predetermined and generated dynamically based on users' regular activities captured by smartphones. Specifically, the constantly changing information about the daily behavior (e.g., phone calls, location traces) of a person is used to create one-time authentication questions (e.g., Who did you call around 4:30 pm today?, What apps did you choose in the last 24 h?). Such dynamic security questions have many potential blessings over static challenge questions. For instance, as dynamic security questions are generated on the fly, users do not have to be compelled to piece these queries earlier .Also, while few static security questions are often not applicable for some users (e.g., What is the name of your 1'st pet?), or may be easily found by searching at someone's Facebook or LinkedIn profile (e.g., "What year did you graduate from college?"), dynamic security questions are likely to be harder to guess by mining online sources due to the randomness of a person's smartphone usage behavior and day-to-day activities.

1.1 Objective

The objective of this thesis is to design a dynamic knowledge based authentication system, taking advantage of the data of smartphone and apps without violating the user privacy. It designs a user authentication system with a set of secret questions created based on the data of users' short-term smartphone usage.

2. BACKGROUND AND RELATED WORK

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% questions can be guessed by the "significant others" who were mainly participants' spouses (77%) and close friends (17%). Another similar study was conducted by Podd et al, which revealed a higher rate of successful guessing (39.5%) [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 .However, today's mainstream secret question methods fail to meet this requirement. A recent study revealed that nearly 20% 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, 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) .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 .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 function as a decent beginning of using ones' short term activities to make secret questions. Since the smartphone has become one's most indivisible device of recording his life, this paper presents a smartphone based autobiographical authentication system. Meanwhile, We evaluate the attack robustness of using a combination of the many light-weight questions (true/false, multiple-choice) rather than exploiting the blank-fillings, so as to strike a balanced tradeoff between security (and/or reliability) and usability.

3. SYSTEM OVERVIEW

The smartphone based autobiographical authentication system consists of two major components, namely the user-event extraction scheme and the challenge-response protocol.

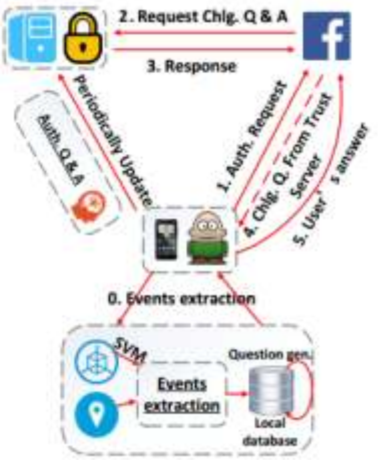

Fig-1 The smartphone based Autobiographical Authentication System[6]

Data Collection: We developed an Android application that supports devices running Android 2.3 or higher to collect autobiographical user data, and then analyzes the collected data to generate challenge questions. Table 1 lists the details regarding the data that are collected in the study.

The communication data (call, SMS) was obtained from the recent communication history. The app usage data is collected from the installed app in the smartphone. Battery charging events were collected when the smartphone was connected to a power source. In order to obtain the location information with minimal energy overhead, I utilize the latest Google Fused Location API. Calendar events are also examined.

Table 1: Details of Collected Data

Data	Details of collected data
Call	Type (outgoing, incoming), duration, name of the person, time, date
SMS	Type (sent, received), receiver/sender name, date, time
App usage	App name, install date, update date
Battery charging	Date, time, mode, percentage
Location	Latitude, longitude, name, date, time
Calendar	Event start date, event end date, event start time, event end time, event description

Questions Generated based on Communication Activity: Communication questions are generated based on a user's recent communication history This category of questions asks a user to answer the name of the person he/she called or SMS messaged, or the name of the person who called him/her or SMS messaged him/her at a specific time.

Questions Generated based on Application Usage Data: We obtain a list of third-party apps via Android API, and also monitor the usage of these apps. After that, it can generate a true/false question like the legacy app: "Did you install/use some app on your phone (in the past few days)".

Questions Generated based on Battery Charging Events: Questions that are generated based on recent battery charging events ask a user to identify the time when the device was plugged into a power source (i.e., charger) within the last 24 hr.

Questions Generated based on Location Information: Location questions are generated based on a user's recent location tracked by the application. The collected location data is consist of a sequence of coordinates with latitude, Longitude.

Questions Generated based on Calendar Events: The questions derived from the calendar events is like "Is there an item planned for next week in your calendar?".

3. CONCLUSIONS

Many web applications provide secondary authentication methods, i.e., secret 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. The widespread presence of smartphones has granted new opportunities to use smartphones to form customized secret questions without violating the user's privacy and security concerns. In this paper, we present a Secret-Question based Authentication system, called "Autobiographical Fallback Authentication Using Smartphones". We created a set of questions based on the data related to sensors and apps, which reflect the users' short-term activities and smartphone usage. The secret questions related to calendar, app installment, and part of legacy apps (call, SMS) 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. Finally, users were found to be positive in general towards the idea of using dynamic security questions for fallback authentication instead of static security questions.

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.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[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 SOUPS., 2009

[6] Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions Peng Zhao, Kaigui Bian, Tong Zhao, Xintong Song, Jung-Min "Jerry" Park, Xiaoming Li, Fan Ye, Wei Yan , IEEE Transactions on Mobile Computing, 16(2), 552–565,2016