Enhancing Security of Secret Question by Using Smart-Phone Sensor

[1]Prof. V. A. Hiray, [2]Avhad Priyanka, [3]Mali Nikita, [4]Pawar Kiran, [5]Sonaje Nikhil

[1]Assistant Professor, [2,3,4,5]BE Computer
Computer Engineering Department,
Shatabdi College of Engineering, Nashik, Maharashtra, India.

***Abstract*:** Many web applications provide secondary authentication methods, i.e., secret questions (or password recovery questions), to reset the account pass-word 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, we present a Secret-Question based Authentication system, called \SecretQA",that creates a set of secret questions on basic of people's smartphone usage. We develop a prototype on Android smartphones, 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 c time and location, Smart Location Reminder is a boon. To serve the purpose, implementing an application for Android-based smartphones and tablets which is not only time based but also location based

***Introduction* -** Secret questions (a.k.a password recovery questions) have been widely used by many web applications as the secondary authentication method for reset-ting the account password when the primary credential is lost. 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. The user can reset his account password by providing the correct answers to the secret questions later.For the ease of setting and memorizing the answers, most secret ques-tions are blank- llings (a.k.a. ll-in-the-blank, or short-answer questions), and are created based on the long-term knowledge of a users personal his-tory that may not change over months/years (e.g., Whats the model of your rst car?). However, existing research has revealed that such blank- lling questions created upon the users 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 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 pro les. An acquaintance of a user can easily infer the answers to the users secret questions (e.g., name of pet). Moreover, a stranger can gure out the answers leaked from public user pro les 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 memorabilitythe required ef-fort or di culty of memorizing the correct answer. Without a careful choice of a blank- lling 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.The recent prevalence of smartphone has provided a rich source of the users 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 ones short-term personal history (typically within one month) for creating his secret question?

LITERATURE SURVEY

When the Password Doesn't Work: Secondary Authentication for Websites [1]

Robert Reeder

et all, In this Nearly all websites that maintain user-speci c 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 assem-bling an arsenal of mechanisms that meet users' security and reliability needs.

User authentication by cognitive passwords: an empirical assessment [2]

M. Zviran

et all, The concept of cognitive passwords is introduced, and their use as a method to overcome the dilemma of passwords that are either di cult 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 ndings of an empirical investigation focusing on memorability and ease-of-guessing of cognitive passwords, are reported. They demonstrate that cognitive passwords are easier to recall than conventional passwords, while being di cult for others, even those close to the users, to guess.

Cost-e ective computer security: Cognitive and associative passwords [3]

J. Podd

et all, Recall and guessing rates for conventional, cognitive, and word associ-ation passwords were compared using 86 Massey University undergraduates. Respondents completed a questionnaire covering all three password types, re-turning two weeks later for a recall test. Each respondent also nominated a "signi cant other" (parent, partner, etc.) who tried to guess the respondent's answers. On average, cognitive items produced the highest recall rates (80%) but the guessing rate was also high (39.5%). Word associations produced low guessing rates (7%) but response words were poorly recalled (39%). Never-theless, both cognitive items and word associations showed su cient promise as password techniques to warrant further investigation.

Its no secret. measuring the security and reliability of au-thentication via secret questions [4]

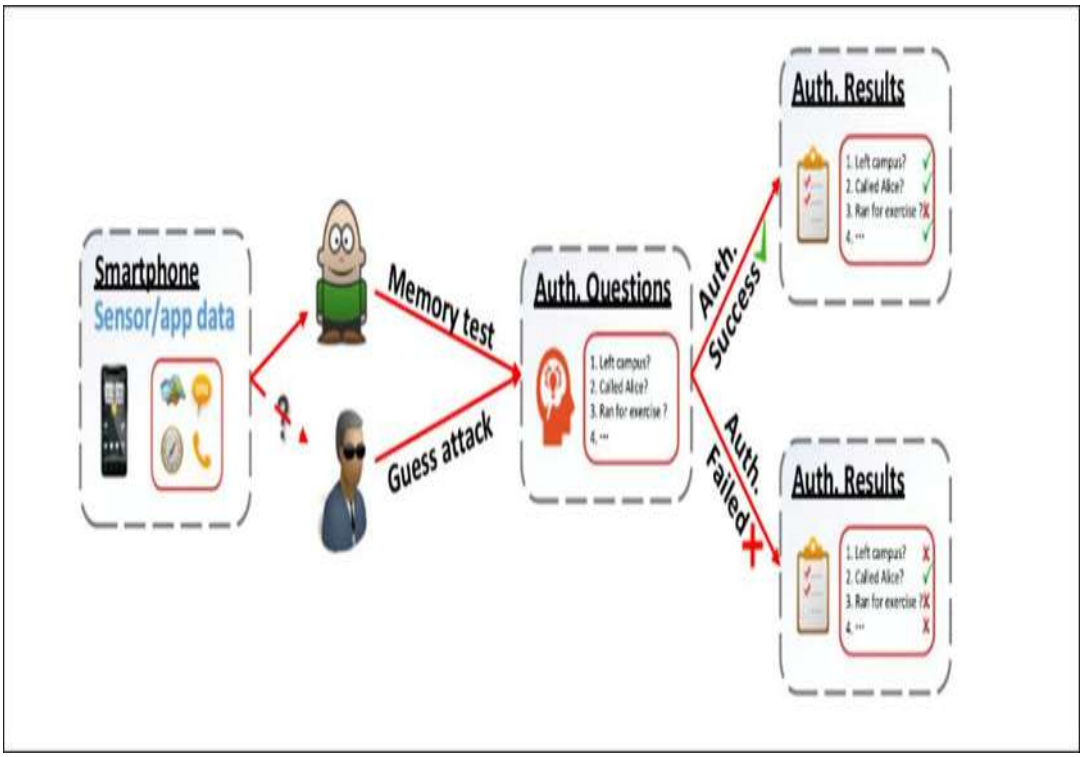
S. Schechter

et all, All four of the most popular webmail providers - AOL, Google, Mi-crosoft, and Yahoo! - rely on personal questions as the secondary authentica-tion secrets used to reset account passwords. The security of these questions has received limited formal scrutiny, almost all of which predates webmail. We ran a user study to measure the reliability and security of the questions used by all four webmail providers. We asked participants to answer these questions and then asked their acquaintances to guess their answers. Ac-quaintances with whom participants reported being unwilling to share their webmail passwords were able to guess 17% of their answers. Participants forgot 20% of their own answers within six months. What's more, 13% of answers could be guessed within ve attempts by guessing the most popular answers of other participants, though this weakness is partially attributable to the geographic homogeneity of our participant pool.

Popularity is everything: A new approach to protecting pass-words from statistical-guessing attacks [5]

S. Schechter

et all, We propose to strengthen user-selected passwords against statistical-guessing attacks by allowing users of Internetscale systems to choose any password they wantso long as its not already too popular with other users. We create an oracle to identify undesirably popular passwords using an ex-isting data structure known as a count-min sketch, which we populate with existing users passwords and update with each new user password. Unlike most applications of probabilistic data structures, which seek to achieve only a maximum acceptable rate false-positives, we set a minimum acceptable false-positive rate to confound attackers who might query the oracle or even obtain a copy of it



The proposed System overcome the drawbacks of authentication precess in real time. We develop a prototype on Android smartphones, 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. Our experimental results reveal that the secret questions related to motion sensors, calendar, app install-ment, 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.

Existing System

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.

Proposed System

The proposed System overcome the drawbacks of authentication process in real time. We develop a prototype on Android smartphones, 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. Our experimental results reveal that the secret questions related to motion sensors, calendar, app instalment, 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.

CONCLUSION

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 secu-rity of secret questions without violating the users privacy. We create a set of questions based on the data related to sensors and apps, which re ect the users short-term activities and smart phone usage. We measure the reliabil-ity 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 perfor-mance 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-e ective 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] [5]. S. Schechter, C. Herley, and M. Mitzen-macher, 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, pp. 200203.