ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.5

To Enhance the Security of Quick Response Code in Smartphones

Dhivya .H[1], P.Vijayasarathy[2]
PG Student[1], Assistant Professor[2]
Department of Computer Science & Engineering
Krishnasamy College of Engineering & Technology, Cuddalore, Tamil Nadu, India

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 (CNP). 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. And also provide a secure system for barcode-based visible light communication for online payment system using image stenography methodology. Secret-Question based Authentication system, called "Secret-QA" that creates a set of secret questions on the basis of people's smartphone usage. To develop a prototype on Android smartphones, and evaluate the security of the secret questions by asking the acquaintance/stranger who participate in user study to guess the answers with and without the help of online tools meanwhile observe the questions reliability by asking participants to answer questions.

Keywords: code, recovery, secret-QA, security.

I. INTRODUCTION

Online shopping is the retrieval of product information via the Internet and issue of purchase order through electronic purchase request, filling of credit or debit card information and shipping of product by mail order or home delivery by courier.
1. Identity theft is the common danger of online shopping.
2. Identity theft is the stealing of someone's identity in the form of personal information and misuse of that information for making purchase.
The concept of text based steganography and visual cryptography using visible light communication, which minimizes information sharing between consumer and online merchant but enable successful fund transfer from consumer's account to merchant's account thereby safeguarding consumer information and preventing misuse of information at merchant side. Secret questions (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. 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 case of setting and memorizing the answers, most secret questions are blank-fillings (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 (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. The Secret-QA system consists of two major components, namely the user-event extraction scheme and the challenge-response protocol. Mobile security or mobile phone security has become increasingly important in mobile computing. Of particular concern is the security of personal and business information now stored on smartphones. More and more users and businesses employ smartphones as communication tools, but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Different security counter-measures are being developed and applied to smartphones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps. Security questions came into widespread use on the Internet. As a form of self-service password reset, security questions have reduced information technology help desk costs. By allowing the use of security questions online, they are rendered vulnerable to keystroke logging attacks. In addition, whereas a human customer service representative may be able to cope with inexact security answers appropriately, computers are less adept. As such, users must remember the exact spelling and sometimes even case of the answers they provide, which poses the threat that more answers will be written down, exposing them to physical theft. Due to the commonplace nature of social-media, many of the older traditional security questions are no longer useful or secure. It is important to remember that a security question is just another password.

II. 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 [6]. 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, 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. QR code (Quick Response Code) is the trademark for a type of matrix barcode (or two-dimensional barcode) first designed for the automotive industry in Japan. A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store data; extensions may also be used. The QR code system became popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. Applications include product tracking, item identification, time tracking, document management, and general marketing. A QR code consists of black squares arranged in a square grid on a white background, which can be read by an imaging device such as a camera, and processed using Reed–Solomon error correction until the image can be appropriately interpreted. The required data are then extracted from patterns that are present in both horizontal and vertical components of the image. QR codes have become common in consumer advertising. Typically, a smartphone is used as a QR code scanner, displaying the code and converting it to some useful form (such as a standard URL for a website, thereby obviating the need for a user to type it into a web browser). QR code has become a focus of advertising strategy, since it provides a way to access a brand's website more quickly than by manually entering a URL. Beyond mere convenience to the consumer, the importance of this capability is that it increases the conversion rate (the chance that contact with the advertisement will convert to a sale), by coaxing interested prospects further down the conversion funnel with little delay or effort, bringing the viewer to the advertiser's website immediately, where a longer and more targeted sales pitch may lose the viewer's interest. QR codes are used over a much wider range of applications, including commercial tracking, entertainment and transport ticketing, product and loyalty marketing (examples: mobile couponing where a company's discounted and percent discount can be captured using a QR code decoder which is a mobile app, or storing a company's information such as address and related information alongside its alpha-numeric text data as can be seen in Yellow Pages directory), and in-store product labeling. It can also be used in storing personal information for use by organizations. An example of this is Philippines National Bureau of Investigation (NBI) where NBI clearances now come with a QR code.

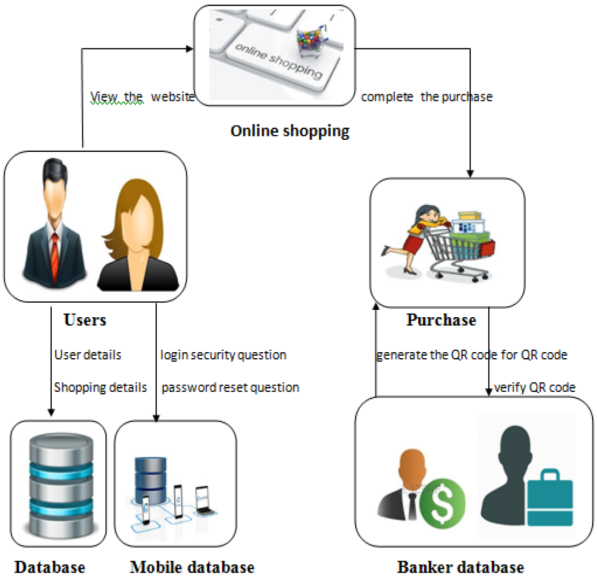


Figure.1. System Architecture

III. SYSTEM OVERVIEW

The User-event Extraction Scheme Today's smartphones 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.

Selection of sensors/apps In the user-event extraction scheme, Secret-QA selects a list of sensors and apps for extracting the user activities, including: (1) the common sensors equipped on the top-ten best-selling smartphones in 2013, the top-ten downloaded Android apps in 2013, and [3] the legacy apps (Call, Contact, SMS, etc.).Because these sensors and apps are already built-in for almost all the smartphones, our approach is naturally suitable for smartphone users without introducing any extra hardware costs.

Secret-QA client app 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. The client app schedules the feature extraction process periodically, and then features will be recorded in the local databases. For example, we adopt libSVM on Android to detect motion related user events, and we set the minimum duration to 10 minutes for noise removal (details on how to create questions and algorithms for other types of events extraction. Note that our extraction of user events are most lazily scheduled using Android Listener [1] 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, 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.

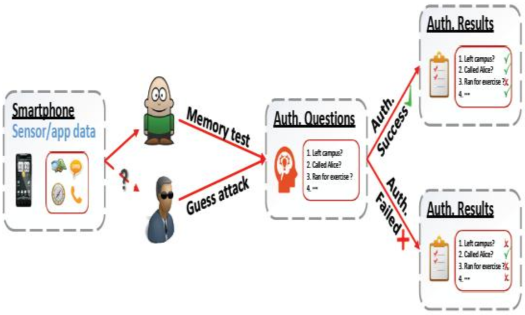
Issue: the user issues an authentication request to the service provider, then the OSN website asks our trusted server for one or more encrypted secret questions and its answers; the questions are finally transferred to the user displaying on the smartphones . The information at this phase must be sent over a secure channel [17] 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 .

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.

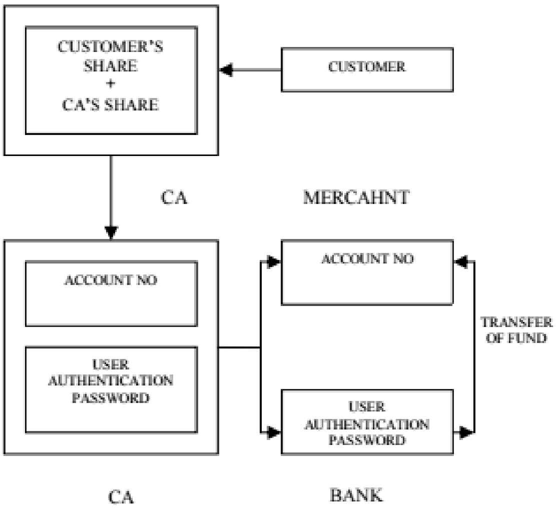
Monitor Phone For Security Question

Monitoring our mobile phone data in order o increase the security. This process was separated into 3 phases they are Application data, Phone status and battery status. If user forgets the password question will be raised phone app like battery status or app status etc. If user gives right answer he will be allowed to change the password. Monitoring our mobile phone data in order to increase the security. This process was separated into 3 phases they are application data, phone status and battery status. If user forgets the password question will be raised phone app like battery status or app status etc. If user gives right answer he will be allowed to change the password.



Transaction In Online Shopping: In this module traditional online shopping consumer selects items from online shopping portal and then is directed to the payment page. Online merchant may have its own payment system or can take advantage of third party payment systems such as PayPal, pay online system, Web Money and others. In the payment portal consumer submit his or her credit or debit card details such as credit or debit card number, name on the card, expiry date of the card.

Image Stenography For Secure Transaction Through Visible Light Communication: Steganography is the art of hiding of a message within another so that hidden message is indistinguishable. The key concept behind steganography is that message to be transmitted is not detectable to casual eye. Visual Cryptography (VC) is a cryptographic technique based on visual secret sharing used for image encryption. Using k out of n (k, n) visual secret sharing scheme a secret image is encrypted in shares which are meaningless images that can be transmitted or distributed over an untrusted communication channel. Only combining the k shares or more give the original secret image. Information submitted by the customer to the online merchant is minimized by providing only minimum information that will only verify the payment made by the said customer from its bank account. This is achieved by the introduction of a central Certified Authority (CA) and combined application of steganography and visual cryptography. The information received by the merchant can be in the form of account number related to the card used for shopping. The information will only validate receipt of payment from authentic customer.


CUSTOMER'S SHARE + CA'S SHARE
CUSTOMER
CA
MERCAHNT
ACCOUNT NO
USER AUTHENTICATION PASSWORD
ACCOUNT NO
TRANSFER OF FUND
USER AUTHENTICATION PASSWORD
CA
BANK

IV. DESIGN OF CHALLENGE-RESPONSE PROTOCOL

We create three types of secret questions: A "True/false" question is also called a "Yes/No" question because it usually expects a binary answer of "Yes" or "No"; a "multiple-choice" ques-tion or a "blank-filling" question that typically starts by a letter of "W", e.g., Who/Which/When/What (and thus we call these two types of questions as "W" questions). We have two ways of creating questions in either a "Yes/No" or a "W" format: (1) a frequency-based question like “Is someone (Who is) your most-frequent contact in last week?”; and (2) a non-frequency based one like “Did you (Who did you) call (Someone) last week?”. Note that the secret questions created in our system are example questions that we have for studying the benefits of using smartphone sensor/app data to improve the security and reliability of secret questions. Researchers are free to create more secret questions with new question formats or by using new sensor/app data, which leads to more flexibility in the design of a secondary authentication mechanism.

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 partici-pants [18], [19] 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 [20], and thus we determine a participant leaves the campus when the GPS location is 500 meters out of the campus area. **Motion activity (accelerometer) related questions**. The example question related to ac-celerometer is No. 2 “Did you do running exercise for at least 10min with your phone carried yesterday?”. There are many smartphone applications that help users to monitor their running activities. We can tell whether the participant is involved in running exercise using the accelerom-eter data, and in order to remove noise, we roughly set the minimum duration of detecting a user’s involvement in running to be 10 minutes [21]. **Smartphone usage (calendar, battery and camera) related questions**. The questions derived from the calendar events is No. 3 “Is there an item planned for next week in your calendar?” As requested by participants, we only recorded whether there would be an item planned in next few days in the calendar; we did not access the content of any planned item in the calendar as it is a severe invasion of privacy. We use the similar format to generate true/false questions related to battery charging and camera usage using Android API: “Did you do something with battery/camera in the past one or few days?” (Question No. 4 and 5 in Table II). **Questions on legacy app usage: contact, call, SMS**. We generate true/false questions related to contact, call, SMS in a similar way. For example, No. 7 question is: “Is *someone* in your contacts on the phone?”. True/false questions can be generated based on call and SMS history using the similar format: “Did you call/text someone?”. Similar to other true/false questions, the correct answer to this question is randomly set as true or false with an equal probability. If the correct answer is set as “true”, we randomly pick a name in the phone’s contact, and replace “someone” in the question with this chosen name literally. Otherwise if the correct answer is set as “false”, we create a fake name to replace “someone” in the question by the approach proposed by Luo *et al* [22]. This approach randomly picks a first name and a last name in phone’s contact list, without colliding with an existing name in the list. **Questions on third-party app instalment and usage**. We obtain a list of third-party apps via Android API, and we also monitor the usage of these apps. We filter out “launcher” apps and EventLog itself in our monitoring experiment. “Launcher” apps are the default home screen applications on Android, e.g., “Samsung Desktop”. As the study [23] indicates, “launcher” apps are the most frequently called ones on Android systems, while users may not be aware of their unintentional usage of it. After that, we can generate a true/false question like the legacy app: “Did you install/use some app on your phone (in the past few days)?”.

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, a true/false questions can be easily extended to be a “W” question: “who did you call/text?” (incoming and outgoing calls/SMS were treated equally), 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. For example, as for Question No. 28 “Who did you call last week?” , we randomly pick a name in participant’s last week call records, and the rest three are faked by names in the contact (meanwhile not appearing in the call records), then we randomly shuffle these names to be the options of the question. We count the number of calls (or SMS) from/to every contact, or the number of times an app is used by a participant, for creating the frequency-based question, e.g., No. 34 “Who was your most frequent contact last week?”. If there are more than one most frequent contacts or most frequently used apps, any answer within these candidates is considered correct. **Answers to blank-filling questions**. For each blank-filling question, we have a default correct answer that is set by our system, as well as an answer input by the participant in the memory test. We use the following method to determine whether an input answer matches the default correct one. First, we can easily filter out futile answers, and then we borrow the approach proposed by Stuart Schechter *et al* [4] to compare the input and default answers, i.e., to remove all non-alphanumeric characters, force letters into lower cases, and allow one error (an improved version of edit distance cost) for every five characters in the default answer.

C. Definition and Thresholds of Determining A Good Question

A *good* secret question is defined as *easy-to-remember* and *hard-to-guess*, i.e., the majority of participants in the memory test could correctly recall the answer, and attackers could not significantly increase their chance more than a random guess.

We set the threshold of easy-to-remember questions to be 80% for both true/false and multiple-choice questions—i.e., 80% participants to correctly answer the question, according to the threshold used for traditional webmail secret questions [4].

V.CONCLUSION

Security questions have reduced information technology help desk costs. By allowing the use of security questions online, they are rendered vulnerable to keystroke logging attacks. The application will be having security question based on their application data and sensor data which are stored in the local database. This makes the attacker a difficult job to crack the security level and reach the application. Every interaction between the user and an intermediate helping device is visualized using a QR code. The authentication key will be send to the smartphone by the intermediator. Finally, QR code and the key will be verified to complete the online transaction. By asking secret question, data can be more secured when sharing highly confidential data like sharing banking details etc.

VI. REFERENCES

[1]. Clark J. and P. van Oorschot P. (2013) “Sok: Ssl and https: Revisiting past challenges and evaluating certificate trust model enhancements,” in Security and Privacy (SP) , pp. 511–525.

[2]. Falaki H., Mahajan R., Kandula S., Lymberopoulos D., Govindan R., and Estrin D., (2010) “Diversity in smartphone usage,” in MobiSys. New York, NY, USA: ACM, pp. 179–194.

[3]. Kim H., Tang J., and Anderson R.,(2012) “Social authentication: harder than it looks,” in Financial Cryptography and Data Security. Springer, pp. 1–15.

[4]. Oner M., Pulcifer-Stump J.A., Seeling P., and T. Kaya T.,(2012) “Towards the run and walk activity classification through step detection-an android application,” in EMBC. IEEE, pp. 1980–1983

[5]. Peng Zhao, Kaigui Bian, Tong Zhao, Xintong Song, Jung-Min “Jerry” Park, Xiaoming Li, Fan Ye, Wei Yan (2016), Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions, pp.99.

[6]. Reeder R . and Schechter S.(2011) “When the password doesn’t work: Secondary authentication for websites,” S & P., IEEE,vol. 9, no. 2, pp. 43–49.

[7]. Roy N., H. Wang H., and Choudhury R.,(2014) “ Am a smartphone and I can tell my user's walking direction”, in Proc. ACM MobiSys, pp.329–342.

[8]. Schechter S., Brush A.B. and S. Egelman S.(2009) “It’s no secret. measuring the security and reliability of authentication via secret questions,” in S & P., IEEE. IEEE, pp. 375–390.

[9]. Schechter S., Herley C., and Mitzenmacher M.,(2010) “Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks,” in USENIX Hot topics in security, pp. 1–8.

[10]. Wang C., Wang Q., Ren K., and Lou W.,(2010) “Privacy-preserving public auditing for data storage security in cloud computing,” in INFOCOM, pp. 1–9.

[11]. M. Dong, T. Lan, and L. Zhong, “Rethink energy accounting with cooperative game theory,” in Proceedings of the 20th Annual International Conference on Mobile Computing and Networking, ser. MobiCom ’14. New York, NY, USA: ACM, 2014, pp. 531–542. [Online]. Available: http://doi.acm.org/10.1145/2639108.2639128.

[12]. R. Faragher and P. Duffett-Smith, “Measurements of the effects of multipath interference on timing accuracy in a cellular radio positioning system,” Radar, Sonar Navigation, IET, vol. 4, no. 6, pp. 818–824, December 2010.

[13]. “Android service api introduction,” Google Android API, 2014. [Online]. Available: http://developer.android.c om/reference/ android/app/Service.html

[14]. A. Drozd, S. Benford, N. Tandavanitj, M. Wright, and A. Chamberlain, “Hitchers: Designing for cellular positioning,” in Proceedings of the 8th International Conference on Ubiquitous Computing, ser. UbiComp’06. Berlin, Heidelberg:

[15]. Springer-Verlag, 2006, pp. 279–296. [Online]. Available: http://dx.doi.org/10.1007/11853565 17

[16]. L. Nyberg, L. B¨ ackman, K. Erngrund, U. Olofsson, and L.-G. Nilsson, “Age differences in episodic memory, semantic memory, and priming: Relationships to demographic, intellectual, and biological factors,” The Journals of Gerontology Series B: Psychological Sciences and Social Sciences, vol. 51, no. 4, pp. P234–P240, 1996.

[17]. W. Luo, Q. Xie, and U. Hengartner, “Facecloak: An architecture for user privacy on social networking sites,” in CSE, vol. 3. IEEE, 2009, pp. 26–33.

[18]. H. Falaki, R. Mahajan, S. Kandula, D. Lymberopoulos, R. Govindan, and D. Estrin, “Diversity in smartphone usage,” in MobiSys. New York, NY, USA: ACM, 2010, pp. 179–194.

[19]. “Top 15 most popular social networking sites until march 2014,” eBizMBA, 2013. [Online]. Available: http://www.ebizmba.com/articles/social-networking-websites