ISSN: 2319-6505

Available Online at http://journalijcar.org

International Journal of Current Advanced Research
Vol 5, Issue 10, pp 1366-1368, October 2016

RESEARCH ARTICLE

International Journal of Current Advanced Research

ISSN: 2319 - 6475

TO ENHANCE THE SECURITY VIA LIGHT-VISIBLE COMMUNICATION IN SMARTPHONES

Dhivya H and Saranya V.S

Krishnasamy College of Engineering & Technology, Cuddalore, Tamil Nadu

ARTICLE INFO

Article History:

Received 9th July, 2016
Received in revised form 5thAugust, 2016
Accepted 28th September, 2016
Published online 28th October, 2016

Key words:

QR code, recovery, secret-QA, security.

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 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 we observe the questions reliability by asking participants to answer their own questions.

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[1].

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 ease 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?")[2]. 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.

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

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. 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 to save battery [4]. 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.

Fig1 System Architecture diagram

Monitor Phone for security question

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.

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.

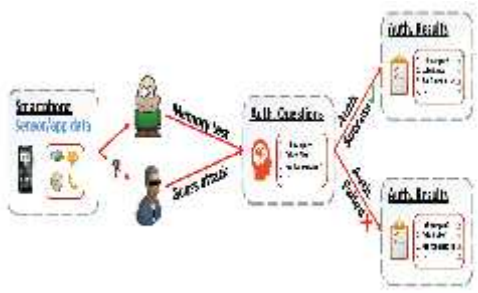

Fig 2 Monitoring secret questions

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" question or a "blank-filling" question that typically starts by a letter of "W", e.g., Who/Which/When/What. 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?",B.)

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[5][6].

Image steganography 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 [7][8]. Only combining the k shares or more give the original secret image.

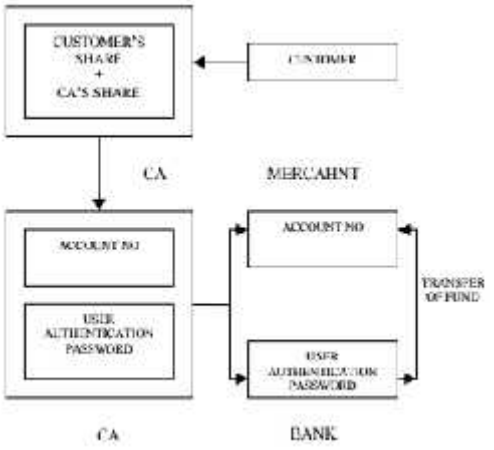

Fig.3 Transaction sample

In the proposed solution, information submitted by the customer to the online merchant is minimized by providing only minimum information, this will verify the payment made by the 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.

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. 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. Therefore by asking secret question, data can be more secured when sharing highly confidential data like sharing banking details etc.

References

1. Peng Zhao, Kaigui Bian, Tong Zhao, Xintong Song, Jung-Min "Jerry" Park, Xiaoming Li, Fan Ye, Wei Yan, *Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions*, pp.99, 2016.
2. 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.
3. H. Kim, J. Tang, and R. Anderson, Social authentication: harder than it looks, in *Financial Cryptography and Data Security*. Springer, 2012, pp. 1–15.
4. M. Oner, J. A. Pulcifer-Stump, P. Seeling, and T. Kaya, *Towards the run and walk activity classification through step detection-an android application*, in *EMBC*. IEEE, 2012, pp. 1980–1983.
5. 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.
6. S. Hemminki, P. Nurmi, and S. Tarkoma, "Accelerometer-based transportation mode detection on smartphones," in *Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems*, ser. SenSys '13. New York, NY, USA: ACM, 2013, pp. 13:1–13:14. [Online]. Available: http://doi.acm.org/10.1145/2517351.2517367
7. 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.
8. N. Roy, H. Wang, and R. R. Choudhury, *I am a smartphone and I can tell my user's walking direction*, in *Proc. ACM MobiSys*, 2014, pp.329–342.

****