International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 2 (March '2017)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

SECURITY ENHANCEMENT OF SECRET QUESTIONS USING USERS SMART PHONE BEHAVIOR

Ramya.R,
Assistant Professor,
Department of Computer Science Engineering,
Jeppiaar SRR Engineering College,
Chennai, India.

Soundarya lakshmi.K,
Student,
Department of Computer Science Engineering,
Jeppiaar SRR Engineering College,
Chennai, India.

Sowndharya.S,
Student,
Department of Computer Science Engineering,
Jeppiaar SRR Engineering College,
Chennai, India.

Abstract: Implementation of application as hacker detection and identification and prevention of important app access in smart phone. The application access can be prevented by the users secret questions given at the time of user registration. The main drawback of existing system is that, the user fined it difficult to remember such secret questions and it can also be hacked by the hacker. In order to overcome the difficulty of such static questions, dynamic questions are generated based on user Smartphone behavior. If the hacker is trying to access the application means system will query the user with 4 random questions (2 – from normal questions and 2 from user runtime pattern. If not authorized then camera, GPS & Voice recorder is initiated and sent as SMS alert and mail to the original user for tracking. SVM algorithm is used for user identification.

Keywords: Secret questions, GPS, SMS Alert, SVM.

I.INTRODUCTION

There exist so many applications in smart phones now days, which includes some confidential applications such as e-shopping, e-banking, e-billing etc. All smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses inherent in smartphones that can come from the communication mode—like Short Message Service (SMS, aka text messaging), Multimedia Messaging Service (MMS), wifi, Bluetooth and GSM, the *de facto* global standard for mobile communications. There are also exploits that target software vulnerabilities in the browser or operating system. And some malicious software relies on the weak knowledge of an average user.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.

Most of the users use smart phone to share their personal and business information for communication. These application access need to prevented from the unauthorized users or from the hackers. Users use pass code or pattern for locking their application. In 2010, researcher from the University of Pennsylvania investigated the possibility of cracking a device's password through a smudge attack (literally imaging the finger smudges on the screen to discern the user's password). The researchers were able to discern the device password up to 68% of the time under certain conditions. Outsiders may perform over-the-shoulder on victims, such as watching specific keystrokes or pattern gestures, to unlock device password or pass code. In order to enhance security for these applications, secret questions are generated. Secret questions includes some set of static and dynamic questions. Static questions are generated at the time of registration and dynamic questions will be generated at the time of user login to the application. These static and dynamic questions are combined and gives as secret questions to the user to check the authorization of the user.

II.RELATED WORK

Guessing attacks by associates and outsiders: The security of secret questions for authentication is given by Zviran and Haga in 1990 [1], which demonstrates that 33 percent of the secret questions are guessed by the unknown persons, 77 percent of the questions are answered by spouses and 17 percent f the questions are answered by the user's close friends. Another study conducted in the same way indicates that the highest rate of guessing secret question is 39.5 percent [2]. A study conducted recently reveals that the question created by the user itself is still liable to the guessing attacks by acquaintance [3].

Poor preciseness of secret questions in real world: a secret question should be memory wise reliable to the user [5]. A recent study states that most of the users above 20 percent

forget their password within six month [3]. Recent proposals for user's security: to reduce guessing attacks by outsider, dynamic questions are generated, namely network activities, physical events and conceptual opinions [6]. For better reliability, user can select secret questions that are easy to elicit than the one that is too difficult to recall [7]. These recent proposals serves a good start for using dynamic questions as secret questions for the betterment of the user. These questions are generated in true/false or multiple choice question to improve the robustness of the password.

III.IMPLEMENTATION

To provide security for sensitive applications pass code and pattern locks are used in existing system. If the user forgets the password a static question which is given at the time of registration will be generated for the user for resetting the pin. However, there is a great chance for the user to forget the password. in order to overcome that dynamic questions and static questions are generated as static questions for the user. If the can able to answer these secret questions correctly, the login will be successful. If the answer was wrong, the application will obatain the user as unauthorized user and captures the image of the user, records the voice, and tracks the location of the user and SMS alert to the alternative number and mail it to the original user.

In case, if the phone went missing, the user can send message to their mobile number from alternative number as "track", which in turn initializes the process automatically and send the unauthorized user's photo, voice and GPS location to the original user as SMS and mail. If the IMSI number was changed, then the application will automatically initializes the process and send alert to the authorized user. SVM algorithm is used for user identification.

III.SYSTEM ARCHITECTURE

In this design, first the user have to register with their own e-mail id and alternate number (IMSI and IMEI number of the phone will be registered automatically after installing the app). Some secret questions such as user's personal information will be registered as static questions for password recovery. When the pin is set successfully, the application will start monitoring the behavior of the phone like last call, last time charged, etc.

When the user login to the particular application to which the lock was set, it will ask for the pin. If the pin war given correctly, then the login will be successful. If the pin was given wrong for more than three to four times secret questions are generated. If the user answers the questions correctly, then the user can login successfully. if the answers are wrong then the application assumes the user as the unauthorized user and captures the image of the user, records their voice and tracks the location of the user and sends notification to the original user's alternative number and mail. Here, SVM algorithm is used for user identification.

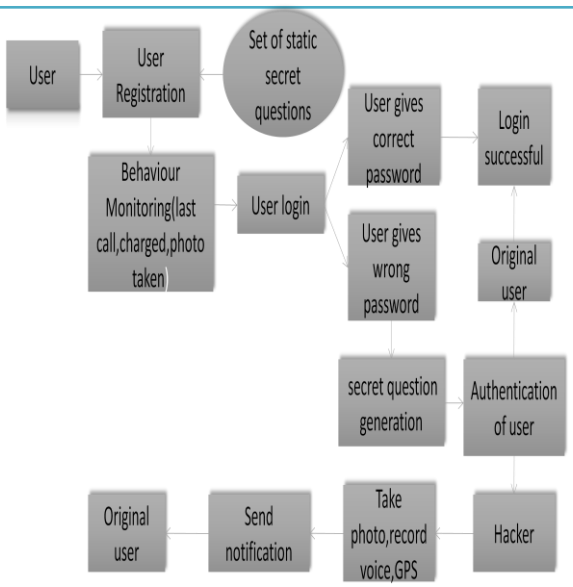

Figure 1: System architecture

IV.METHODS

1. User Registration with Some Standard Questions: User details are registered with the fields like username, password, and personal details with some set of questions and answers. These details are saved and application start monitoring the user behaviour for dynamic data.

2. Server Authentication: The Server Application which is used to communicate with the Mobile Clients. The Server can communicate with their Mobile Client by GPRS and GPS. User will be initially registering with the server. Server also will maintain last activities of the phone like which time you put in charger and last call in your phone and some gallery photos etc..If the pass code given by the user is wrong then the server will check for the authorization of the user.

3.Runtime Analysis : Secret questions that are registered at the time of registration and monitored by the server are generated as set of static and dynamic questions to the user. If the answers given by the user are wrong, the server assumes that the user is the unauthorized person and intimate it to the original user.

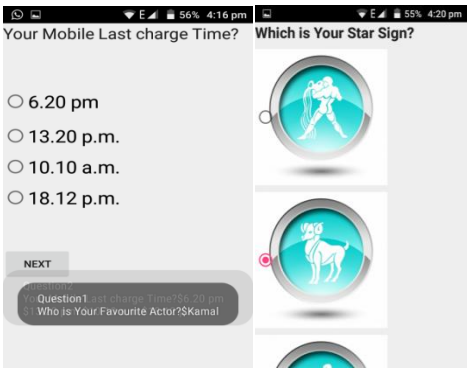

Figure 2: Secret question generation.

IV.IDENTIFICATION OF HACKER

The image ,voice recorded, GPS location of the unauthorized user will be sent via E-mail and SMS to the original user.The

same process will be initiated when the server detects the change of IMSI number of the phone.

V.RESULTS

In this application the authorized user can recover their pass code by answering static and dynamic questions in the form of multiple choice questions easily and an unauthorized user can be detected and identified by the original user without any delay. It captures the unauthorized user and find their location and intimate it to the original user which in turn makes the original user to identify the unknown user instantly.

VI.CONCLUSION

In this paper secret questions based security has been implemented and conduct a user study that how much data collected by Smartphone behaviours can enhance the security of secret questions without violating the users privacy. In the future system applications can be developed by recording the users hand waving pattern and the dynamic questions can be generated using this pattern.

REFERENCES

[1]. 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.
[2]. 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.
[3]. 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.
[4]. 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.
[5]. 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.
[6]. A. Babic, H. Xiong, D. Yao, and L. Iftode, "Building robust authentication systems with activity-based personal questions," in ProcSafeConfig. 2009, pp. 19–24.
[7]. H. Kim, J. Tang, and R. Anderson, "Social authentication: Harder than it looks," in Proc. 16th Int. Conf. Financial Cryptography DataSecurity, 2012, pp. 1–15.