ISSN (Online): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3 Issue.6 June 2017

Systematic Design for Highly Secure Smartphone Application

Lavanya.S[1], Karthikeyan.R[2]

[1] PG Student, Department of Computer Science Engineering, Mohamed Sathak Engineering College, kilakarai.

[2] Associate Professor & Head, Department of Computer Science Engineering, Mohamed Sathak Engineering College, kilakarai.

Abstract – **In recent years' web application provides the secret questions for that time of user's login failure. Secondary authentication method i.e. secrete question is the most invited feature in web applications. But smart phone application faces the security is major challenging issue during this time of access the secondary authentication method which provides some secret question, however these secrete question can easily have guessed by other persons. It affects the reliability in smart phone application. Our proposed method designs for overcome existing problems such as security and reliability of secondary authentication method in smart phone application. Here we design the Secret question based Authentication system [SECRET-QA]. In SECRET- QA system, we set the three secret questions with specified time, user can answer the question only within the time otherwise we cannot access the application by this method we secure the user smart phone application. Our method set the secret questions based on following categories such as location based, recent activities such as short term mobile phone usage therefore we secure our smart phone application from unauthorized user. Because our proposed method sets the three secret questions are sessional varied manner, so other persons could not easily answer the answers. Here we evaluate the reliability and security of secret questions.**

Index Terms – **Mobile Security, Wireless Sensor Network, Smart Phone GPS, Android (OS)**

I. INTRODUCTION

Authentication is the act of confirming the truth of an attribute of a single piece of data [a datum] requested true by an entity. In difference with identification which mentions to the act of stating or otherwise indicating a claim supposedly attesting to a person or thing's identity, authentication is the procedure of actually confirming that identity. It might involve confirming the identity of a person by verifying the authenticity, validating their identity documents of a website with a digital certificate, defining the age of an artifact by carbon dating, or else ensuring that a product is what it's packaging and labeling claim to be. In other words, authentication often includes confirming the validity of at least one form of identification. Authentication is used by a server when the server needs to know exactly who is accessing their information or site.

Authentication is used by a client when the client needs to distinguish that the server is system it claims to be. In authentication, the user or computer has to prove its identity to the server or client. Usually, confirmation by a server involves the use of a user name and password. Other ways to authenticate can be over cards, voice recognition, retina scans, and fingerprints. Authentication by a client typically includes the server giving a certificate to the client in which a trusted unauthorized user such as VeriSign or else Thawte conditions that the server belongs to the entity such as a bank that the client expects it to. Authentication does not control what responsibilities the separate can do or what files the individual can see. Authentication just identifies and checks who the person or else system

Mobile security or else mobile phone security has become progressively important in mobile computing. Of particular anxiety is the security of personal and business information now stored on smart phones more and more users and businesses employ smart phones as communication apparatuses, but also as a incomes of preparation and establishing their work and private life. Within companies, these machineries are producing profound variations in the organization of information systems and therefore they have become the source of new risks. Indeed, smart phones collect and compile an increasing amount of sensitive information to which access must be organized to protect the privacy of the user and the intelligent property of the corporation.

All smart phones, by way of computers, are favored targets of attacks. These attacks deed faintness connected to smart phones that can come from incomes of communication like Short Message Service [SMS, text messaging], Multimedia Messaging Service [MMS], Wi-Fi networks, GSM and Bluetooth, the de facto global systematic for mobile communications. There are also attacks that exploit software susceptibilities from both the web browser and operating system. Finally, there are forms of malicious software that rely on the weak information of average users.

Different security counter measures are existence established and applied to smart phones, from security in different layers of software to the distribution of information to end users. There are good achieves to be observed at all levels, from design to use, finished the development of operating systems, downloadable apps and software layers, A smart phone user is unprotected to several threats when they use their phone. In just the last two quarters, the number of exclusive mobile threats grew by 261%, according to ABI Research. These threats can disturb the process of the smart phone, and communicate or else change user data. For these reasons, the applications deployed there must guarantee privacy and integrity of the information they handle. In accumulation, meanwhile some apps could themselves be malware, their functionality and activities should be limited for example, restricting the apps from accessing position information via GPS, blocking access to the user's address book, preventing the transmission of data on the network, sending SMS messages that are billed to the user, etc..There are three prime targets for attackers:

Data: smart phones are devices for data management; so they may comprehend sensitive data like credit card numbers, authentication information, private information,

activity logs such as calendar, call logs. Identity: smart phones are highly customizable, so the device or its contents are associated with a precise person. For illustration, every mobile device can transmit information related to the owner of the mobile phone contract, and an attacker may want to take the individuality of the owner of a smart phone to obligate other crimes;

Accessibility:

By attacking a smart phone one can bound access to it and remove the owner of the service. The sources of these attacks are the same performers originate in the non-mobile computing space: Specialists, whether profitable or else military, who attention on the three boards stated above. They steal penetrating data from the general public, as well as undertake manufacturing cleverness. They will also use the individuality of those attacked to achieve other attacks; Thieves who want to gain revenue finished data or identities they must stole. The thieves will attack many people to increase their potential income; Black hat hackers who specifically attack availability. Their aim is to develop worms, and reason damage to the device. In some cases, hackers have an attention in stealing data on devices Old hat hackers who reveal vulnerabilities. Their aim is to expose susceptibilities of the device. Old hat hackers do not intend on harmful the device or else pilfering data.

Mobile application management [MAM] defines software and services accountable for provisioning and supervisory entrance fee to inside develop and commercially accessible mobile apps used in business settings on both corporations providing and transport your personal smart phones and tablet computers. Mobile application management provides rough controls at the application equal that enable administrators to manage and secure app data. MAM differs from mobile device management [MDM], which focuses on controlling the entire device and requires that users enroll their device and install a service agent. While some enterprise mobility management [EMM] suites include a MAM function, their capabilities may be incomplete in comparison to stand-alone MAM clarifications because EMM suites require a device management outline in order to enable app management competences. Any security questions or else identity information accessible to users to reset forgotten passwords should preferably have the following four features:

Memorable:

If users can't remember their answers to their security questions, you have achieved nothing.

Consistent:

The user's answers should not change over time. For instance, asking "What is the name of your significant other?" may have a different answer 5 years from now.

Nearly universal:

The security questions should put on to a wide a spectators of possible.

Safe:

The answers to security questions should not be somewhat that is easily guessed, or else research [e.g., something that is matter of public record] our proposed work provides the security for smart phone applications with sets the three secret questions the questions are setting based on location and shot time mobile usage.

II. SYSTEM STUDY

The first technique requires the organization to create a library of predefined challenge questions. During enrollment, a user selects a subset of these questions and enters their own answers. The second technique requires the user to create their own challenge questions and provide the answers to these questions during enrollment. A third technique involves the use of challenge questions derived from private information databases. This approach asks the user personal questions, such as what company services your current mortgage" or "what the balance on your previous bill was. Some organizations prefer to use a third party service to compile and provide access to this information rather than managing it themselves. In this scenario, the user does not initially select or answer any challenge questions since this information has already been gathered. Based on our experience, the first and second techniques are most popular for use with online authentication. Organizations may prefer these techniques over the third approach due to their lower cost. Of the two main challenge question approaches, Security PS recommends that organizations use the first and create a predefined library of questions for their users.

We believe that most users will create unsatisfactory challenge questions on their own and, accordingly, should not be allowed to do so. In part, this is because we have seen organizations make little effort to educate users on how to come up with good challenge questions. However, even security professionals scuffle to create good challenge questions, so education of users alone isn't sufficient. More analysis of the problems with user defined challenge questions can be found in the Security PS blog. Once the challenge questions are selected and answers are provided, the user can complete the enrollment process. When the user returns to use the application, these test questions may or may not be asked depending on how the authentication system was implemented. In many cases, challenge questions are used in conjunction with a password for authentication. Users can be prompted to answer challenge questions during every login or only under specific conditions. Certain risk-based authentication (RBA) systems only present challenge questions when the user logs in from a different computer.Users can be prompted to answer challenge questions in one of two ways. A user can either type in their answer free-form or they can select their answer from the multiple choices presented by the authentication system.

When required to type their answer, a user's greatest challenge is remembering the exact answer provided during enrollment. If they cannot remember their answer they must blindly submit guesses or contact the organization to reset their questions. In this respect, challenge questions with free-form answers are similar to passwords. Our proposed method overcome

the above issues in secret question authentication system by using SCRET-QA authentication system

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 reliability) and usability.

A. *Mobile security*

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 smart phones.

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. Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

All smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smartphones that can come from means of communication like Short Message Service (SMS, aka text messaging), Multimedia Messaging Service (MMS), Wi-Fi networks, Bluetooth and GSM, the de facto global standard for mobile communications. There are also attacks that exploit software vulnerabilities from both the web browser and operating system. Finally, there are forms of malicious software that rely on the weak knowledge of average users.

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.

B. *Wireless network*

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes

Wireless networking is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.[2] Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.[3]

Examples of wireless networks include cell phone networks, Wireless local networks, wireless sensor networks, satellite communication networks, and terrestrial microwave networks.

C. *Wireless sensor network*

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass

their data through the network to a main location. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

D. Android

Android is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touch screen mobile devices such as smartphones and tablets. Android's user interface is mainly based on direct manipulation, using touch gestures that loosely correspond to real-world actions, such as swiping, tapping and pinching, to manipulate on-screen objects, along with a virtual keyboard for text input. In addition to touch screen devices, Google has further developed Android TV for televisions, Android Auto for cars, and Android Wear for wrist watches, each with a specialized user interface. Variants of Android are also used on notebooks, game consoles, digital cameras, and other electronics.

Android has the largest installed base of all operating systems (OS) of any kind. Android has been the bestselling OS on tablets since 2013, and on smartphones it is dominant by any metric.

Initially developed by Android, Inc., which Google bought in 2005, Android was unveiled in 2007 along with the founding of the Open Handset Alliance – a consortium of hardware, software, and telecommunication companies devoted to advancing open standards for mobile devices. As of July 2013, the Google Play store has had over one million Android applications ("apps") published – including many "business-class apps" that rival competing mobile platforms – and over 50 billion applications downloaded. An April–May 2013 survey of mobile application developers found that 71% of developers create applications for Android, and a 2015 survey found that 40% of full-time professional developers see Android as their priority target platform, which is comparable to Apple's iOS on 37% with both platforms far above others. In September 2015, Android had 1.4 billion monthly active devices.

Android's source code is released by Google under open source licenses, although most Android devices ultimately ship with a combination of open source and proprietary software, including proprietary software required for accessing Google services. Android is popular with technology companies that require a ready-made, low-cost and customizable operating system

for high-tech devices. Its open nature has encouraged a large community of developers and enthusiasts to use the open-source code as a foundation for community-driven projects, which deliver updates to older devices, add new features for advanced users or bring Android to devices originally shipped with other operating systems. The success of Android has made it a target for patent (and copyright) litigation as part of the so-called "smart phone wars" between technology companies.

III. USER EVENT EXTRACTION MODULE

Our proposed method provides the security for smart phone applications by using SECRET-QA authentication system. In SCRET- QA authentication system first designs the user event extraction module which extracts the information from user smart phone applications. The extracted information based on recent activities of user such as short term usage of smart phone applications and location of user. Our method sets the secret questions based on this user event extraction module. By using this module, we set the three secret questions for each smart phone applications.

IV. CHALLENGE RESPONSE PROTOCOL

Our proposed method sets the secret questions by using challenge response protocol module which provides the more security for smart phone applications. Here we set the three secret questions based on information collected by user event extraction module for each smart phone application and each question has separate time. User should answer the question only within the specified time if user not answer the question within the time we cannot access the smart phone applications. By this method we provide the security from other persons.

V. PERFORMANCE EVALUATION

Here we provide the security by the setting of three secret questions for each smart phone applications. By this method we improve the reliability in secondary authentication system. Our proposed method provides the more security from unauthorized user by setting the time for each secret question. Here we evaluate the performance of SCRET-QA system by the parameter of reliability

VI. ALGORITHM DESCRIPTION

Our proposed work provides the security for smart phone application by the designing of SECRET-QA authentication system. SECRET –QA system sets the secret questions for smart phone applications which provide the security for smart phone applications. Here our proposed work SECRET-QA system set the secret questions based on recent activities of user and location information of user. In SECRET- QA system has two phases first user event extraction and challenge response protocol, user event extraction phase extracts the user event such as recent activities of user which can capture by the smart phone sensor applications and location information which is also captured from the sensor applications of smart phone.

In second phase challenge response protocol sets the secret questions based on user event extraction. Here we sets the three secret questions with time basis, each questions have a specified answering time user should answer the question only within specified time. If user answer the question within time can access the application otherwise user cannot access the application. SECRET QA system sets the secret question sessional varied manner therefore other persons could not access easily. By this method we improve the system reliability and security in smart phone applications.

VII. CONCLUSION AND FUTURE WORK

Our proposed work presents the security of user smart phone application by using the system SECRET-QA authentication system. By this system we provide the three security question for each smart phone application. SECRET-QA first extracts the user event which based on recent activities of user and location of user from smart phone applications. From this extracted information our challenge response protocol phase sets the secret question in server. Here we provide the specified answering time for each question user should answer the question only within the time otherwise user could not access the application due to this method our proposed system more reliable and provide secure from other persons. Since other person does not guess the answers correctly within the time. Our proposed method analyze the performance of SECRET-QA system by the parameter reliability. Here we provide the security of smart phone application by setting of three secret questions with time basis it leads the computational complexity. In future we have to planned for design the single secret question authentication system and provide the more reliability in single secret question system. In addition we analyze the performance evaluation with various parameters such as usability and reliability.

REFERENCES

[1] 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, IEEE, 1990, pp. 137–144

[2] 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, 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 S & P., IEEE. IEEE, 2009, pp. 375–390.

[4] I. Craik and R. S. Lockhart, "Levels of processing: A framework for memory research," Journal of verbal learning and verbal behavior, vol. 11, no. 6, pp. 671–684, 1972.

[5] Babic, H. Xiong, D. Yao, and L. Iftode, "Building robust authentication systems with activity-based personal questions," in SafeConfig. New York, NY, USA: ACM, 2009, pp. 19–24.

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

[7] 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.

[8] 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.

[9] D. A. Mike Just, "Personal choice and challenge questions: A security and usability assessment," in *SOUPS*. 2009.

[10] A. Rabkin, "Personal knowledge questions for fallback authentication: Security questions in the era of Facebook," in SOUPS. ACM, 2008, pp. 13–23.