Virtual OS of Semi-Authorized in a Smartphones

Moceheb Lazam Shuwandy

[1]Sultan Idris Education University, Faculty of Art, Creative Computing Industry, Perak, Tanjung Malim, Malaysia
[2]CCMS, TU, IQ

Abstract: ***Identity theft is one of the biggest challenges to protecting electronic devices, especially in protecting Smartphones. Authentication and its techniques are the most vulnerable to problems, such as traditional, pattern password and PIN code etc. In addition, biometric techniques are safer than normal authentication methods. Therefore, these techniques are related to the characteristics of human beings and used to authenticate who owns them. Besides, authentication is granted by an Operating System OS to protect authentication data onto theft and manipulation. However, local OS s are vulnerable to problems such as hacker attacks, and systems and Multi-trying to enter the device when it stole. On the other hand, the connection to the OS should be available when requesting authentication in a Smartphone, otherwise the user will not be able to access his device. In this paper, we discuss the failure connected to OS in order to obtain authentication, and some cases lead to non-authentication. We are discussing the user's access to the Smartphone by any biometric devices currently in use. When using of the virtual OS if the OS fails to determine the real Authorized, by creating a Virtual OS (VOS) on the Smartphone. For example: a user cans only access to his device, when obtain on the Authorized form of VOS. It has the same specifications and environment, as the original OS.***

Keywords: Virtual OS, Authentication, Local OS, Semi-Authorized, Smartphone**.**

1. Introduction

The biometric verification procedures, for example: face detection, retina scanning or fingerprint are viewed as more secure than the contemporary confirmation components, for example: smart card technology, even pattern locks, PIN or passwords in the cell phones. Regular verification instruments including graphical or alphanumeric passwords require that the client recalls the special blend of secret key. Additionally, the secrecy of the secret key is likewise a noteworthy worry in security frameworks. Secret key or PIN based verification instruments can likewise be broken by utilizing estimate or Brute Force dictionary [1-6]. Biometric validations give enhanced unwavering quality and ease of use in light of the fact that dissimilar to traditional techniques, it needs not to be recollected. Biometric procedures are either ordered as physiological (i.e. scanning of retina or fingerprint and so forth.) or behavioural, for example, voice. Additionally, Signature of Handwritten has a place with behavioural biometrics. It is one of the most established and most broadly utilized strategies for a person authentication on a document [8].

In different hands, the OS exhibit is an appropriated application structure that bundles assignments or workloads between the providers of an advantage or organization, called Operating System, and organization requesters called an Authorized. Much of the time customer and OS pass on finished a mobile phone orchestrate on autonomous hardware, be that as it may, both customer and OS may live in a comparable structure. An OS has to keep running no less than one OS programs which share their benefits with customers. A customer does not share any of its advantages but instead requests an OS's substance or organization work. Customers, henceforth, begin correspondence sessions with OS s which envision moving toward requesting. Instances of PDA applications that use the OS show is Email, a mastermind to print, and the Internet [11].

This paper aims to allow people who either have lost their ability empowered to reach smartphone unauthorized persons trying to access data across multiple ways, to give them a recipe on a semi-authorized by virtual operating system. The smartphone connects to the OS before using a secure authentication. The system of successful operation begins from Smartphone, the user access to his cell phone depends on one of security methods built in it. For example, some using one of the biometric technologies then it sends a request to the OS, the OS receives the data of authentication and makes process with a Database. The Database checks the data, Is available for this smartphone or not? After the OS confirms that the authentication exists and matches what it has in the database, it returns the answer to the smartphone to allow the user to use the device. All this keeps the smartphone waiting for an OS response, from request to response. See the figure 1 below.

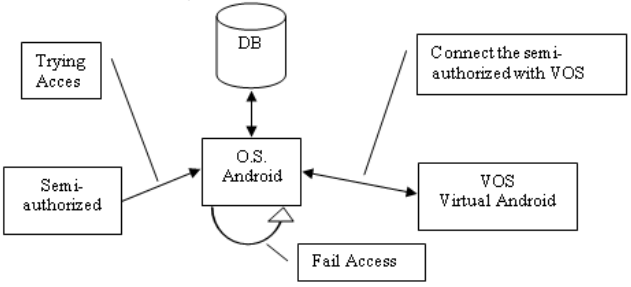

Figure 1: Show Semi-authorized connect to VOS in successful Authentication

2. Significant of Study

S It is important to maintain the interest of the user for the purpose of continuing to use the product. In this paper, we seek to discuss the problem and the solution. The faulty connection to the Local OS to obtain authentication or vice versa will prevent the Authorized ized user from using his or her phone. For example, if someone uses the fingerprint, the smartphone will send the authentication request to the OS. Which means that the person will be in a state of waiting until the response comes from the OS. A person may be an elderly person, a patient, a child, a doctor, a banker, etc. In addition to keeping the connection to the OS at any time and the continuity of user access to the device and uphold the security of the smartphone [6-9].

The connection of the smartphone to Local OS for the purpose of allowing the client to use it and determine whether it is authorized or not, is more security in terms of security. But the problem is in the first three directions to the OS and the second in the response of the OS and the third in the carrier. The delay caused by any of the above three reasons does not guarantee as semi-Authorized. The person Authorized access to his system freely. Any security method, if feasible, is a failure.

3. Literature view

The verification information was blended with the protected information that was gathered all the while with the technique sort that utilized some time recently. It was watched that keep information in a memory of individuals in addition to the inconvenience that happens while overlooking the information is not a superior approach to genuine approve [6]-[8]. Or, on the other hand, assault from who need to get to a gadget. Confirmation data made it safe in faraway [7], [8], utilizing an OS to spare the data in the Data base. The trial was performed by volunteers who conveyed cell phone amid interface OS. Another researcher was done to particularly recognize the direction of cell phone grabbing by utilizing one of the kind elements extricated from a Biometric innovation of cell phone. [10]

Some researchers proposed framework engineering in view of three levels. To start with level is the client end. The client utilizes a cell phone to play out his mark noticeable all around. The cell phone is conveyed by the client in his grasp while he plays out the mark. [1]-[4] The data of movement detected by the accelerometer is then sent to the OS for confirmation. [5] OS, which is the second level, applies coordinating calculation to distinguish the client. [11]

4. Objective

The main objective of this paper is to build a temporary local OS that matches the Local OS in performance. The other thing is to keep the authentication outside of the smartphone, which would preserve the data without being able to access it without authentication. Besides, eliminate the loss of time that causes suffering to the user, especially in urgent and emergency situations.

5. Methodology

We discuss a way to solve the above problem, and how to find ways to eliminate the bugs. The system consists of a primary OS and a temporary local OS and a communication process between them. The application to authenticate access to the smartphone connects to the Local OS. The application will not allow the user to try to log in without a prior connection to the OS, which makes it very troublesome if repeated failure to connect.

3.1 Virtual Operating System VOS Successful Connection

VOS has all the specifications of the original OS, plus a small database containing only the authentication data of the smartphone. The application creates the first local OS after the first successful authentication with the Local OS as shown in Figure 2, which explains the process of creating the local OS. As follows:

1) The user uses the smartphone; the application connects to the Local OS.
2) Successful connection.
3) Application The user is required to enter the technical means for the purpose of authentication.
4) The user enters, the smartphone says sending the authentication to the OS for the purpose of matching.
5) The OS receives the request and queries the database about the request.
6) When the process is completed, the OS responds with a successful authentication.
7) Smartphone receives the answer of the OS, and the application opens the device to the user.
8) The application creates the local OS where it saves the successful authentication in the local database after encryption.
9) The connection with the OS is closed after the end of the process of establishing the local OS.

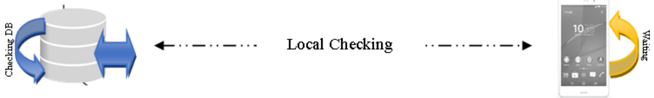

Figure 2: Show Smartphone in failure connection with the Local OS

3.2 Virtual Operating System VOS Unsuccessful Connection

When the Local OS connection fails, the system makes the smartphone:

1) The user uses the smartphone; the application connects to the Local OS.
2) Failed to connect to two attempts.
3) The application connects to the local OS.
4) The connection was successful.
5) Application The user is required to enter the technical means for the purpose of authentication.
6) The user enters, the smartphone says sending the authentication to the OS for the purpose of matching.
7) The OS receives the request with the data after encryption and queries from the database about the request.
8) When the process is completed, the OS responds with a successful authentication.
9) Smartphone receives the answer of the OS, and the application opens the device to the user.

The application tries to connect to the Local OS. When successful, they connect to the local OS, check the data in the local database, and then say to change the internal data code after checking the data. In a case of incorrect login, the application says that the device is shut down until it is entered again correctly. See Figure 3.

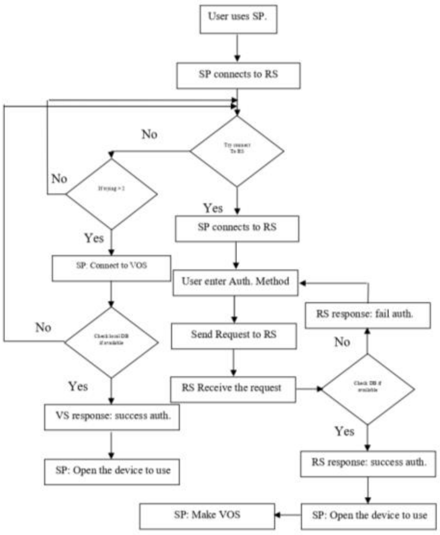

Figure 3: Flowchart show Smartphone (SP) connect to Local OS (RS) and Virtual OS (VOS)

6. Discussion

Some researchers may say “Why do not we skip the Local OS at the local OS?” If we assume that we have done so, we will lose the local OS in the first flaw in the smartphone system. This includes the result of a defect in the operating system or attack from hackers or because of some viruses and then it will cause great damage to the local OS and disrupt the work in addition to absence access to information that was saved. In addition, the loss of the device means the loss of the local OS, which means that the Local authentication is better in many cases can be a future study intended to develop a local OS nearby not in the device itself, but in another device nearby and our study will cover it.

7. Conclusion

We discussed how to address the problem of lost connection between the smartphone and the OS in devices that authenticate Local access. And the development of a mechanism for the purpose of reducing the dependence on the existence of connection to the Local OS or not. However, this solution needs to be applied for the purpose of verifying the feasibility of its use. This depends on the environment and the mechanism used to determine the quality and specifications of all devices used.

References

[1] Aviv, Adam J., et al. "Practicality of accelerometer side channels on smartphones." Proceedings of the 28th *Annual Computer Security Applications Conference*. ACM, 2012.

[2] Derawi, Mohammad Omar, et al. "Unobtrusive user-authentication on mobile phones using biometric gait recognition." 2010 Sixth International Conference on *Intelligent Information Hiding and Multimedia Signal Processing. IEEE*, 2010.

[3] Doroz, Rafal, and Piotr Porwik. "Handwritten signature recognition with adaptive selection of behavioral features." *Computer Information Systems–Analysis and Technologies. Springer*, Berlin, Heidelberg, 2011. 128-136.

[4] Feng, Tao, Xi Zhao, and Weidong Shi. "Investigating mobile device picking-up motion as a novel biometric modality." 2013 IEEE Sixth *International Conference on Biometrics: Theory, Applications and Systems* (BTAS). *IEEE*, 2013.

[5] Laghari, Asadullah, and Zulfiqar Ali Memon. "Biometric authentication technique using smartphone sensor." 2016 13th *International Bhurban Conference on Applied Sciences and Technology (IBCAST)*. IEEE, 2016.

[6] Shuwandy, Moceheb Lazam. "Smile Mask to Capsulation MOLAZ Method." *International Journal of Computer Science and Network Security* (IJCSNS) 13.12 (2013): 66.

[7] Shuwandy, Moceheb Lazam, et al. "Switching between the AES-128 and AES-256 Using Ks* & Two Keys." *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY* 10.8 (2010): 136-140.

[8] Shuwandy, Moceheb Lazam, et al. "Sensor-based mHealth authentication for real-time remote healthcare monitoring system: A multilayer systematic review." *Journal of medical systems* 43.2 (2019): 33.

[9] Vildjiounaite, Elena, et al. "Unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices." *International Conference on Pervasive Computing. Springer*, Berlin, Heidelberg, 2006.

[10] Weiss, Gary M., and Jeffrey W. Lockhart. "Identifying user traits by mining smart phone accelerometer data." *Proceedings of the fifth international workshop on knowledge discovery from sensor data*. ACM, 2011.

[11] Yeh, Kuo-Hui, Nai-Wei Lo, and Yingjiu Li. "Cryptanalysis of Hsiang-Shih's authentication scheme for multi-server architecture." *International Journal of Communication Systems 24.7* (2011): 829-836.

Author Profile

Moceheb Lazam Shuwandy received the B.Sc. degrees in Computer and Software Engineering from Al-Mustansiria University Baghdad – College of Engineering - Department of Computer Engineering and Software 1998-2003, M.Sc. degrees in Information Technology of Utara University of Malaysia – College of Arts and Sciences in 2012 and Ph.D. degrees in Artificial Intelligence of UPSI – FSKIK in 2019. During 2005-2008, he worked as supervisor of the Internet networks in the Tikrit University, Iraq (TUI). In 2005 he served as director of the website of the University of Tikrit, Iraq. In 2006-2017 he worked lecturer in the Faculty of Education / Department of Mathematics and CCMS - University of Tikrit, Iraq in article Visual Studio® J # & C#. He is a member of the Iraqi Engineers Syndicate /Baghdad 2004. He works lecturer (2012-2017) in College of Computer Science, TUI. He worked Associate Dean of the Faculty of

Mathematics and Computer Science for Administrative Affairs from (2015-2017).