International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Security and Privacy Enhancement Framework for Mobile Devices using Active Authentication

S Udith Narayanan, P Vignesh, T Manigandan
Department of Computer Science and Engineering,
G.K.M. College of Engineering and Technology, Chennai, Tamil Nadu, India

ABSTRACT

The techniques we used to develop and to ensure the separation of enterprise content and personal data on an end-user's device. Although the enterprise manages the environment in which work-related activities are conducted, referred to as a work persons third-party applications installed on the mobile devices may make the enterprise content vulnerable to misuse or exfiltration.An application restriction policy is configured through our Application Restriction Manager (ARM) Policy Manager that allows one to set different restrictions for each installed application. Our approach, that we refer to as DroidARM, focuses on post-installation application restriction policies. Such policies dynamically restrict the capabilities of mobile applications at run-time. An application restriction policy is configured through our Application Restriction Manager (ARM) Policy Manager that allows one to set different restrictions for each installed application. Adhering to the policy, our ARM system limits the capabilities of an application by restricting access to data and system resources contained within the work persona. Data shadowing is a data and system resource protection technique we have chosen to leverage. We have implemented DroidARM and integrated it into the Android operating system. Our experimental results show that our approach is efficient and effective.

Keywords: *Text, application usage, web browsing, and location*

I. INTRODUCTION

Main objective of this project is to Mobile Android applications often have access to sensitive data and resources on the user device. Misuse of this data by malicious applications may result in privacy breaches and sensitive data leakage. In our paper, we rely on sensor positioning techniques to retrieve the location of the device. In addition to these techniques, we also set the restrictions of mobile device in login sessions and message passing system to admin control .We introduced the design of our architecture through describing the components of our access control framework with the corresponding role of its entities.

II. RELATED WORKS

The sampling error, question wording and practical difficulties in conducting telephone surveys may introduce some error or bias into the findings of opinion polls.“M. Duggan, “Cell phone activities 2013,” PewResearchCenter, Washington, DC, USA, 2013”. Andreas Saltos, Daniel Smith, Kristin Schreiber, Sarah Lichenstein, Richard Lichenstein (Corresponding author), May 26, 2015(Journal of Safety Studies). The various potential solutions to this problem, one promising technique is mouse dynamics, a procedure for measuring and assessing a user’s mouse behavioral characteristics for use as a biometric.“On the Effectiveness and Applicability of Mouse Dynamics Biometric for Static Authentication: A Benchmark Study”.Chao Shen Zhongmin Cai1, Xiaohong Guan Jialin Wang ,In *Proc. IEEE 5th IAPR ICB*, 2012.The special-character placeholders, some features capture aspects of computer.org/ITPro 3 1 the user’s style usually not found in standard authorship problem settings. “Decision fusion for multimodal active authentication”.A. Fridman et al, *IEEE IT* Professional july 2013. As a result of this, not only phone numbers and addresses are stored in the mobile device but also financial information and business details which definitely should be kept private. “Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recognition”.Mohammad O. Derawi , Claudia Nickel , Patrick Bours and Christoph Busch.In *Proc. IEEE 6th Int. Conf. IIH-MSP*, 2010.

III. PROPOSED SYSTEM

In this paper we have proposed the restriction system for application, there is the application blocking that is internal and external application want to block through the admin panel the particular application connectivity The Administrator has set the privileges to access the persons. The person has no permission to access the restriction apps. She/he cannot access the restriction application, and the menu options with the message passing system into admin panel , the user want to use restriction application for emergency purpose incase user can pass the message into the admin panel , if it’s the valid reason then the administrator can allow to use application for that user. There is extra propose in this, such that the alarm notify the system to remind if the user forget to logout the application. When the person login the application it will be shown in the admin and can restrict. There are also logout options in case if the user logout then the person device cannot control.

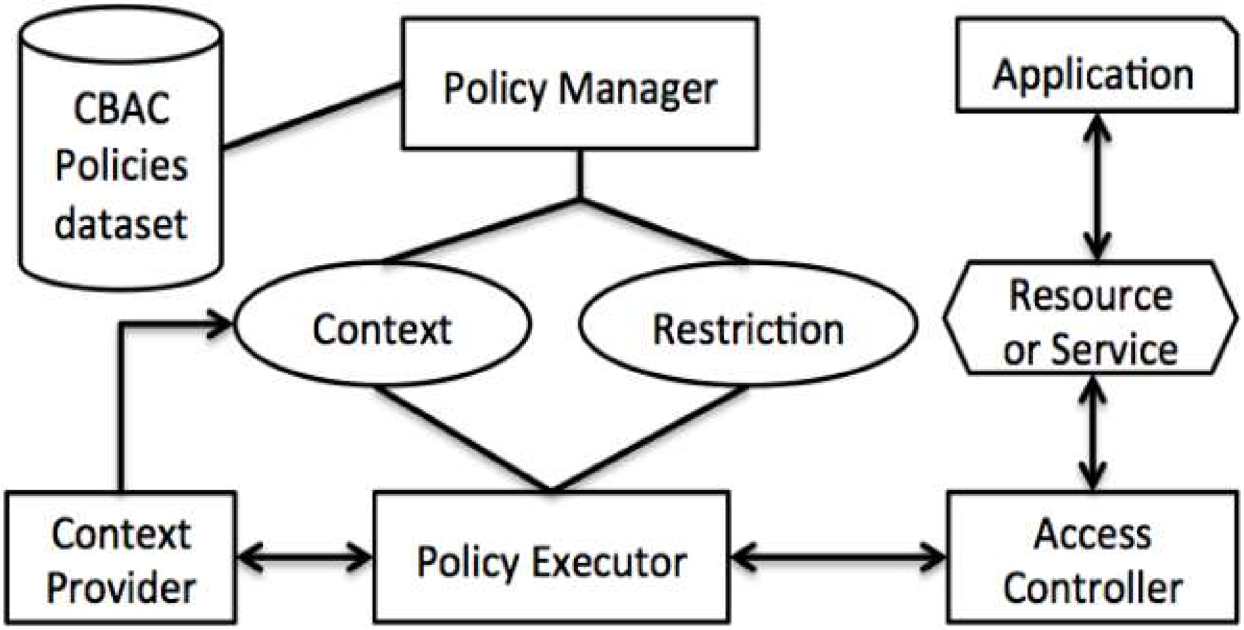

Fig.2 Block diagram of ARS

A. Admin panel creation:

Develop the admin panel using the localhost (wampserver & myphpadmin) and create the default login account for all the application user along with restriction menus.

B. Policy Manager:

The admin can control the android application only if the terms and conditions (policy) are accepted by the android user.

C. Authentication:

The authentication process will be done between the mobile device & admin panel in the login account if and only if login is successful and gets the user permission to access the admin panel.

D. Admin restriction system:

If the user login the account in android mobile it will be shown in the admin panel who are logging in &being in online list only then admin can set the privileges for users.

CONCLUSIONS

In this paper, we proposed parallel binary decision-level fusion architecture for classifiers based on four biometric modalities: text, application usage, web browsing, and location. Using this fusion method we addressed the problem of active authentication and characterized its performance on a real-world data set of 200 subjects, each using their personal Android mobile device for a period of at least 30 days.

REFERENCES

1. "Biometric Authentication Using Wavelet Probabilistic Neural Network".Ching-Han Chen, Ching-Yi Chen2,2013 IEEE 17th International Symposium on Consumer Electronics (ISCE).

2. "Towards Multiple User Active Authentication in Mobile Devices", Mattias Andersson , Hironao Okada, IEEE TENCON 2013 Journal Publication.

3. " Extracting IM evidence of Android apps Sign In or Purchase",Dr. Sridhar Mandapati , Sravya Pamidi , Sriharitha Ambati,Journal of Computer Engineering 2015.

4. "Monitoring Temperature Changes in Body",Abdul Hadi H. Nograles, Felicito S. Caluyo, IEEE INDICON 2013 Journal Publication.

5. "Toward Writing Style Anonymization",Akshata V.S, Rumana Pathan, Poornima Patil, Farjana Nadaf.International Journal of Core Engineering and Management(IJCEM) 2014.