International Journal on Applicationsin Information and Communication Engineering
Volume 2:Issue 6: June 2016, pp 39-42. www.aetsjournal.com ISSN (Online) : 2394 - 6237

Provision of Access Control for Mobile Devices Based on Situation using CBAC Mechanism

D.Geetharani, K.Saravanan

***Abstract*—** Mobile Android applications often have access to sensitive data and resources on the user device. Misuse of data by malicious applications may result in privacy breaches and sensitive data leakage. In order to overcome such privacy problems an access control mechanism is proposed. Mobile applications are increasingly being deployed and used by enterprises, military and other secured industries. As mobile applications have so many advantages but every application comes with issue of data security. Mobile Android applications have access to sensitive data and resources on the user device. Misuse of this data by malicious applications may result in privacy breakage and sensitive data leakage. Protecting this sensitive data from leakage is a critical issue. In android mobile applications, the chances of such critical data leakage will be on higher side. For example, in many applications at the time of installation the application ask for system privileges. The fact is that Android users do not have control over the application capabilities once the applications have been granted the requested privileges upon installation. Mobile devices cannot be protected by physical security the same way as stationary systems can be protected. A large-scale simulation study, using the Linear Road Benchmark and VM performance traces from the AWS public cloud, shows that while GA-based heuristic provides a better quality schedule, the greedy heuristics are more practical, and can intelligently utilize cloud elasticity to mitigate the effect of variability, both in input data rates and cloud resource performance, to meet the QoS of fast data applications.

***Keywords*—** Android, Wi-Fi, Smart phone device, Context Awareness, Context Based Access Control, Mobile Application, Smart phone devices, Security and Privacy.

I. INTRODUCTION

As smart phones are becoming more powerful in terms of computational and communication capabilities, application developers are taking advantage of these capabilities in order to provide new or enhanced services to their applications. For example, on March 2013 Samsung unveiled its Galaxy S4 device with 8 CPU cores and 9 sensors that enrich the device with powerful resources [1]. However, the majority of these resources can collect sensitive data and may expose users to high security and privacy risks if applications use them inappropriately and without the user's knowledge. The threat arises when a device application acts maliciously and uses device resources to spy on the user or leak the user's personal data without the user's consent. Moreover, users carrying their smart phones in public and private places may unknowingly expose their private information and threaten their personal security as they are not aware of the existence of such malicious activities on their devices [2].

Since such a feature is still missing in popular smart phone systems, such as in Android systems, it is crucial to investigate approaches for providing such control to device users. The need for configurable device policies based on context extends from high profile employees to regular smart phone users. For example, government employers, such as in national labs, restrict their employees from bringing any camera-enabled device to the workplace, including smart phones, even though employees might need to have their devices with them at all times as their devices may contain data and services they might need at any time. With context-based device policies, employees may be allowed to use smart phones as they can disable all applications from using the camera and any device resources and privileges that employers restrict while at work, while the user device can retain all its original privileges outside the work area [3-6].

Context-based policies are also a necessity for politicians and law enforcement agents who would need to disable camera, microphone, and location services from their devices during confidential meetings while retaining these resources back in non-confidential locations. With context-based policies, users can specify when and where their applications can access their device data and resources, which reduces the hackers' chances of stealing such data. The danger arises when a device application acts intentionally harmful and uses device resources to keep a watch on user's activities or leak the user's personal data without the user's consent [7].

Moreover, users carrying their Smartphone in public and private places may unknowingly expose their private information and can put their personal security in danger. The smart phone user is not aware of the existence of malicious activities getting performed on their devices. To prevent such harm and leakages, users must be able to have a better control over their device capabilities by reducing certain application privileges while being in public places e.g. At work place, shopping malls [8,9]. To achieve such type of security mechanism, Smartphone systems must provide device owners with configurable policies that enable users to control their device usage of system resources and application privileges according to context, mainly location and time. Since such a feature is still missing in popular Smartphone systems, such as

D.Geetharani, PG Scholar, Computer science and Engineering,Department of CSE, Annai Mathammal Sheela Engineering College, Namakkal.(Email: geetharanids25@gmail.com.)

K.Saravanan, Assistant Professor, Computer science and Engineering,Department of CSE, Annai Mathammal Sheela Engineering College, Namakkal

in Android systems, it is crucial to work on such systems and make them more secure and efficient[10-12].

II. Architectural Design

We studied the some architectures and one of them we are going to implement more efficiently. Studied framework consists of an access control mechanism that deals with access, collection, storage, processing, and usage of context information and device policies. To handle all the aforementioned functions, given framework design consists of four main components. The Context Provider (CP) collects the physical location parameters (GPS, Cell IDs, Wi-Fi parameters) through the device sensors and stores them in its own database, linking each physical location to a user-defined logical location.

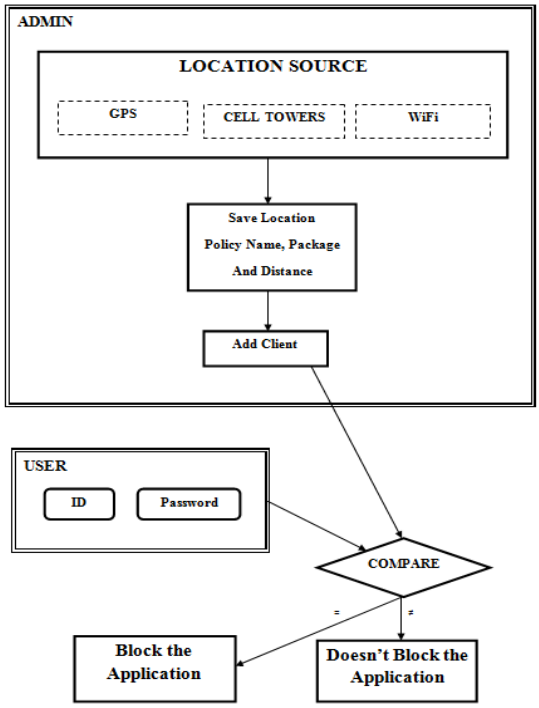

Fig.1 System Architecture

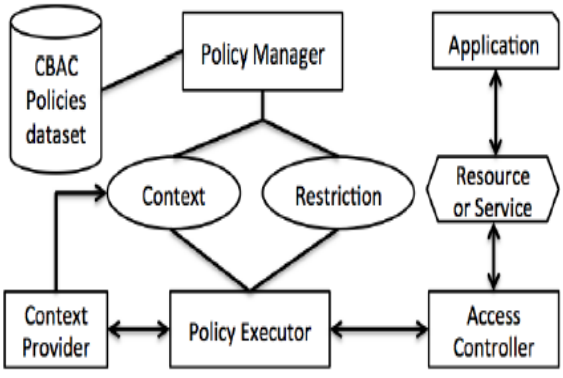

Fig.2 Access Control Framework

It also verifies and updates those parameters whenever the device is re-located. The Access Controller (AC) controls the authorizations of applications and prevents unauthorized usage of device resources or services. Even though the Android OS has its own permission control system that checks if an application has privileges to request resources or services, the AC complements this system with more control methods. The AC enhances the security of the device system since the existing Android system has some permissions that, once granted to applications, may give applications more accessibility than they need, which malicious code can take advantage of.

To introduced the design of our architectures through describing the components of our access control framework, with the corresponding roles of its entities. Our framework consists of an access control mechanism that deals with access, collection, storage, processing, and usage of context information and device policies. To handle all the aforementioned functions, our framework design consists of four main components.

The Context Provider (CP) collects the physical location parameters (GPS, Cell IDs, Wi-Fi parameters) through the device sensors and stores them in its own database, linking each physical location to a user-defined logical location. It also verifies and updates those parameters whenever the device is re-located.

The Access Controller (AC) controls the authorizations of applications and prevents unauthorized usage of device resources or services. Even though the Android OS has its own permission control system that checks if an application has privileges to request resources or services, the AC complements this system with more control methods and specific fine-grained control permissions that better reflect the application capabilities and narrow down its accessibility to resources. The AC enhances the security of the device system since the existing Android system has some permissions that, once granted to applications, may give applications more accessibility than they need, which malicious code can take advantage of. For example, the permission READ PHONE STATE gives privileged applications a set of information such as the phone number, the IMEI/MEID identifier, subscriber identification, phone state (busy/available), SIM serial number, etc.

The Policy Manager (PM) represents the interface used to create policies, mainly assigning application restrictions to contexts. It mainly gives control to the user to configure which resources and services are accessible by applications at the given context provided by the CP. The Policy Executor (PE) enforces device restrictions by comparing the device's context with the configured policies. Once an application requests access to a resource or service, the PE checks the user-configured restrictions set at the PM to either grant to deny access to the application request. The PE acts as policy enforcement by sending the authorization information to the AC to handle application requests, and is also responsible to resolve policy conflicts and apply the strictest restrictions.

III. OVERVIEW

A. Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system.

The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple.

The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations, and steps to follow when error occurs.

B. Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2. Select methods for presenting information.

3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- ❖ Convey information about past activities, current status or projections of the Future.
- ❖ Signal important events, opportunities, problems, or warnings.
- ❖ Trigger an action.
- ❖ Confirm an action.

Input Design is the process of converting a user-oriented description of the input into a computer-based system. The input design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

IV. THE JAVA PLATFORM

A *platform* is the hardware or software environment in which a program runs. We've already mentioned some of the most popular platforms like Windows 2000, Linux, Solaris, and MacOS. Most platforms can be described as a combination of the operating system and hardware. The Java API is a large collection of ready-made software components that provide many useful capabilities, such as graphical user interface (GUI) widgets. The Java API is grouped into libraries of related classes and interfaces; these libraries are known as *packages*.

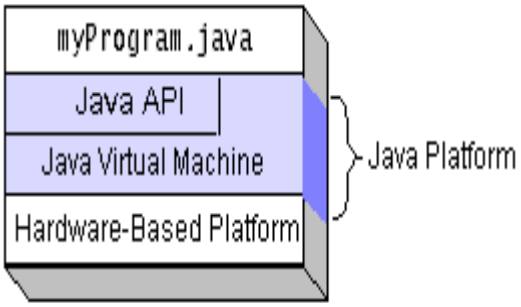

Fig.4.3.3 Program Runs In Java Platform

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

- Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the

V. CONCLUSION

In this paper, an android application has been implemented which support context based access control policies. This will help the application to restrict the malicious data and allow the system to access the specific data and/or resources based on user context. The proposed CBAC mechanism for android systems allows smart phone users to set configuration policies over their applications' usage of device resources and services at different contexts. For example, set of restricted privileges for device applications can be set when using the device at

public place, and device applications may re-gain their original privileges when the device is used at private place.

A. Future Enhancement

The approach requires users to configure their own set of policies the difficulty of setting up these configurations require the same expertise needed to inspect application permissions listed at installation time. The modified versions of the Android OS supporting context-based access control policies. These applications restricts the accessing of specific data and/or resources based on the user context. However we plan to extend the approach to give network administrators of organizations the same capabilities once a mobile device connects to their network. Network administrators are able to block malicious application accesses to resources and services that may affect the security of their network. Approach is critical for assuring security of corporate networks when organizations allow users to "bring their own devices".

REFERENCES

[1] K. Church, B. Smyth. Understanding the Intent Behind Mobile Information Needs. In Proc. 14th Int'l Conf. Intelligent User Interfaces. ACM, 2009: 247-256.
[2] M. Green, S. Hohenberger, and B. Waters. Outsourcing the Decryption of ABE Cipher texts. USENIX Security Symposium. Aug. 2011.
[3] A. Sahai, and B. Waters. Fuzzy Identity-Based Encryption. Advances in Cryptology EUROCRYPT, vol. 3494, 2005.
[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute based Encryption for Fine-grained Access Control of Encrypted Data. In Proc. 13th ACM Conf. Comp. Common. Security, New York, USA, pp. 89–98, 2006.
[5] J.Bethen court, A. Sahai, and B. Waters. Cipher text-policy Attribute based Encryption. In IEEE Symp. Security and Privacy, SP 07. pp. 321–334, May 2007.
[6] K. Zaidi, Y. Rahul amathavan, and M. Rajarajan. DIVA - Digital identity in VANETs: A Multi-authority Framework for VANETs. In Proc. 19th IEEE Int'l Conf. Netw. (ICON'13), Singapore, Dec. 2013.
[7] R. Lu, X. Liang, X. Li, X. Lin, Xuemin Shen, EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications. In IEEE Trans. Parallel and Distributed Systems, vol.23, no.9, pp.1621-1631, Sep. 2012.
[8] F. Li, Y. Rahul mathavan, M. Rajarajan, R. C.-W Phan. Low Complexity Multi-authority Attribute Based Encryption Scheme for Mobile Cloud Computing. In Proc. IEEE 7th Int'l Symp. Service Oriented System Engineering (SOSE), San Francisco, USA, pp. 573–577, Mar. 2013.
[9] F. Li, N. Clarke, M. Papadaki, and P. Dowland. Misuse Detection for Mobile Devices Using Behaviour Profiling. In Int'l Journal of Cyber Warfare and Terrorism, vol. 1, no. 1, pp. 41–53, Jan.–Mar. 2011.
[10] M. Miettinen, P. Halonen, and K. Hatonen. Host-based Intrusion Detection for Advanced Mobile Devices. In Proc. 20th Int'l Conf. Advanced Information Networking and Applications, pp. 72–76, Washington, DC, USA. 2006.
[11] N. Eagle, and A. S Pentland. Reality Mining: Sensing Complex Social Systems. Journal Personal and Ubiquitous Computing, vol. 10, no. 4, pp. 255 – 268, Mar. 2006.
[12] Y. Rahulamathavan, V. Moonsamy, L. Batten, S. Shunliang and M. Rajarajan. An Analysis of Tracking Service Settings in Blackberry 10 and Windows Phone 8 Smartphones, 19th Australasian Conference on Information Security and Privacy (ACISP), Wollongong, Australia, Jul., 2014.
[13] M. Chase. Multi-authority Attribute Based Encryption, In Lecture Notes of Theory of Cryptography in Computer Science, Berlin Heidelberg, pp. 515–534, 2007.
[14] M. Chase, and S. S. M. Chow. Improving Privacy and Security in Multiauthority Attribute-Based Encryption. In Proc. 16th ACM Conf. Comp. Commun. Security, New York, NY, USA, pp. 121–130, 2009.
[15] A. B. Lewko, and B. Waters. Decentralizing Attribute-based Encryption, in EUROCRYPT, ser. LNCS, K. G. Paterson, Ed., vol. 6632. Springer, pp. 568–588, 2011.
[16] C. Burnett, P. Edwards, T. J Norman, L. Chen, Y. Rahulamathavan, M. Jaffray, E. Pignotti. TRUMP: A Trusted Mobile Platform for Selfmanagement of Chronic Illness in Rural Areas. In Trust and Trustworthy Computing, pp. 142–150. Springer Berlin Heidelberg, 2013.
[17] D. Weerasinghe, Y. Rahulamathavan, M. Rajarajan. Secure Trust Delegation for Sharing Patient Medical Records in a Mobile Environment. Health Policy and Technology, vol. 2, pp. 36–44, 2013.
[18] L. Scott, and D. E. Denning. A Location Based Encryption Technique and Some of Its Applications. In Proc. National Technical Meeting of The Institute of Navigation, Anaheim, CA, pp. 734–740, Jan. 2003.
[19] L. Hsien-Chou, and C. Yun-Hsiang, A New Data Encryption Algorithm Based on the Location of Mobile Users, Information Technology Journal, vol. 7, no. 1 pp. 63-69, 2008.
[20] Al-Ibrahim, Omar, Ala Al-Fuqaha, D. V. Dyk, and N. Akerman. Mobility Support for Geo-Encryption. In Proc. IEEE Int'l Conf. Commun., pp. 1492–1496, 2007.
[21] V. Vijayalakshmi, and T. G.Palanivelu. Secure Localization Using Elliptic Curve Cryptography in Wireless Sensor Networks. Int'l Journal of Comp. Sciences and Netw. Security, vol. 8, no. 6 pp. 255–261, 2008.
[22] R. Karimi, M. Kalantari. Enhancing Security and Confidentiality in Location-based Data Encryption Algorithms, Applications of Digital Information and Web Technologies (ICADIWT), 2011 Fourth Int'l Conf., pp. 30–35, Aug. 2011.