International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015
ISSN 2091-2730

Security Profiles for Smart Phones

Pritam R. Tarle, Dr. A. P. Khedkar
Savitribai Phule Pune University, India
prits.tarle@gmail.com, anagha_p2@yahoo.com

Abstract: Increased smart phone usage has raised issues of their security and privacy. This work proposed a system based on mode-of-uses separation in smart phones to provide security profiles for it. This is a software application developed android smart phone that allows user to define and implement security profiles. It provides applications separation and data separation. Profiles are not hardcoded or predefined rather user can define security profiles. Switching between profiles is automatic based on context detection. Rules based security is provided to restrict access to device resource like Bluetooth, Wi-Fi, mobile data, NFC etc. So, other users are restricted from using smartphone resources. Experiments are conducted to observe energy overhead for designed application and to calculate time required for switching of security profiles. Result shows that security profile application does not cause any noticeable overhead.

Keyword*:* Android, Access control, Context, Security, Virtualization

I. INTRODUCTION

Smart phones are playing vital role in our regular life. In the corporate world, smart phones are becoming famous these days. From smart phone user does different functions anywhere anytime with device's high storage and computing speed. Many companies use mobile versions of desktop applications to improve employee productivity by allowing access to company services with smart phones. Many companies are trying the BYOD (Bring Your Own Device) concept. For this, employees connect their personal smart phones to their work place. In such situations, many times, employee has to give his personal phone to other employees for the sake of work and one's personal device gets handled by others. In such cases, no one can guarantee safety of personal data on the device. On the contrary, outside workplace, if any one handles employee's smartphone, company's data stored on that smartphone comes under risk. This may lead to risk of company's confidential data leakages, data losses and data theft etc. Hence securing use of the smart phone and data access control according to different reasons of smartphone use is of the key importance.

Taking security risks related to smart phones into consideration, there is should be some effective and easy to use solution making the use of smart phones secure, as far as the hastily increasing utilization of these devices is considered. Multiple techniques are suggested for securing the data stored on the smart phones. Some of them are android extensions i.e. making change in the android OS. While in some other solutions, mobile virtualization technique is applied. This paper tells about details of implementation of a solution developed for smartphone security using security profiles.

II. RELATED WORK

Many risks associated with smart phones security are identified. Some solutions are suggested and still the experiments are going on. This chapter shows some of the previous research work on smart phone security. Security related techniques for smartphones are mainly divided into following parts as android security extension and mobile virtualizations. Russello, Conti presented a system which consists of security profiles on smartphone. They developed a system called MOSES [1] which separates data and applications in different security profiles. But it does not restrict resource access on device for resources like Bluetooth, Wi-Fi, NFC etc.

A. Android Security Extension

Many solutions have been developed which are android security extensions. CRêPE is a context related policy enforcement system [2]. M. Conti, Crispo developed a fine grained context related policy enforcement. With this user can create policies that automatically control the granting of the permissions during runtime. Context-related access control is not new, but this work used this concept in smart phone environment.

YAASE (Yet Another Android Security Extension) is a very flexible and very powerful privacy enforcement framework [3] transparent to the applications in Android environments. Russello, Crispo have developed an Android security extension by modifying

Android framework, libraries. They implemented a security system for protecting user from various malicious applications. But this system is the modifications of an Android operating system itself. All above solutions are nothing but Android security system extensions i.e. modification of framework of Android OS. Hence, removing these systems will not just as simple as removal of the application and may result in the non working android system.

Flexible data driven security for Android [4] is developed that includes data-driven usage control, and generalization of access controls to the time after data accessed. Feth, Pretschner suggested flexible data driven security for Android. Security policy enforcements are based on event and actions. Policies are built on temporal, spatial, cardinality conditions. But this system assumes non rooted, vulnerability free mobile device. Both assumptions are fairly questionable. The reason for this is that, rooting an android phone is simple even for the unexperienced users and vulnerability reports are pretty frequent.

Other research by Kodeswarn and Nandkumar presented system based on run time information flow control to secure enterprise data on the smart phone [5]. Their privacy policies are based on permissible information flow during different context on phone. But policy conflicts increase with increase in the number of policies.

FlaskDroid [6], is other approach that developed diverse security and privacy policies with flexible and fine grained mandatory access control on Android framework platform. This architecture gives mandatory access control over Android middleware and kernel layers simultaneously. But more flexible policies are required to address attacks.

If a security technique has multiple security policies then, it is necessary to identify the best suitable security policy that should be implemented in a particular scenario. To identify best suitable security policy from multiple policies, optimization technique such as conventional genetic algorithm (GA) [7] can be used. Further GA with novel operators viz. Basic and advanced twin operator can be used for efficiently optimizing the security profiles for accessing mobile applications [8].

B. Mobile Virtualizations

Virtualization gives environments that are partitioned, and indistinguishable from "bare" hardware, from operating system point of view. With the rise of smart phone performance capabilities, virtualization porting to mobile platform became actual. There are some approaches to port Linux hypervisors to the ARM architecture. Xen described design of Xen on ARM, which is a secure system virtualization of ARM [9]. Researchers developed system virtualization for ARM based mobile phones using Xen hypervisor. They isolated secure guest Linux virtual machine from non-secure ones which are executing under Xen hypervisor on ARM. But the system has low performance.

However, all virtual machines are just ported to mobile platforms while being premeditated for PC, they share low performances. Considering android OS security [10], which explained complexity of security of Android and security enforcement and research on security assessment of Android framework for mobile devices [11], researchers identified high risk threats to the framework and suggested some security solutions for mitigating them.

III. SYSTEM ARCHITECTURE

Proposed application which consists of security profiles for smart phones provides security and space isolation based on modes of uses separation on smart phone. Security profiles are nothing but separate compartments which consists of different applications that are assigned to those profiles by user as per his needs. This work also defines rules based security to restrict access to device resource like Bluetooth, Wi-Fi, mobile data, NFC (Near Field Communication) etc. In this work:

- Proposed system separates modes of smartphone use in terms of security profiles.
- Security profile (SP) determines when data can be accessed and what applications can be executed within a profile.
- Within particular SP, only applications assigned to that SP are allowed to execute; this provides application separation.
- Policies are comprised of rules based security. Using rules defined for each SP, access of device resources is controlled for that SP.
- These profiles are associated with a set of contexts which determines the activation of profile.
- Contexts definitions include the use of information like time.
- Profiles can applied any time by the user. Graphical user interface will be provided for this.
  Security profile switching can be manual or automatic as required by user. Automatic switching between the security profiles is possible using context detector system.

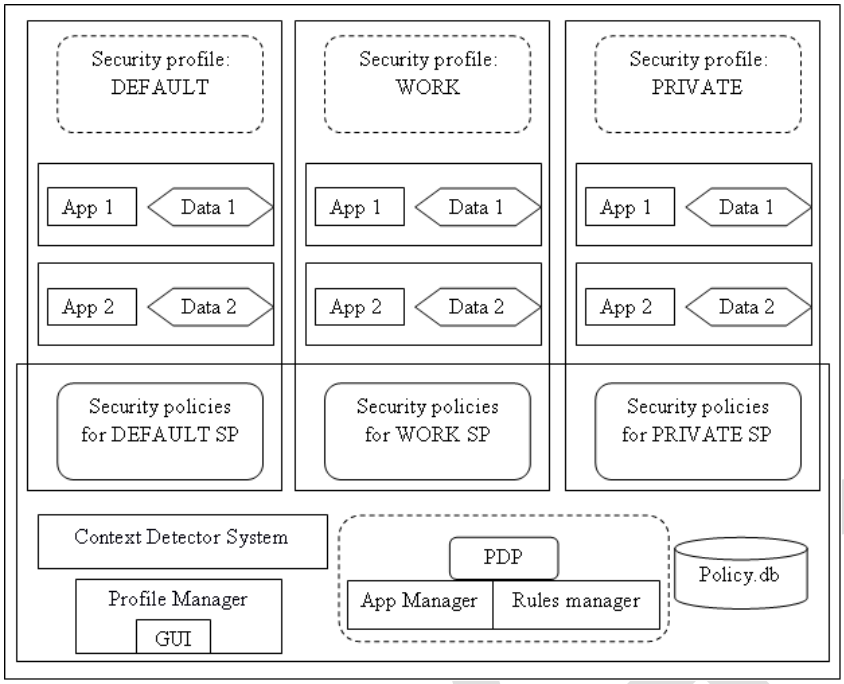

Fig. 1 Proposed Architecture

The Fig.1 summarizes the architecture for the proposed system which describes inter-related functionalities of components of system.

IV. IMPLEMENTATION DETAILS

Proposed system consists of the components presented in above figure. Security profile will be associated with a set of security policies defined for that particular SP. These policies control the access to applications and data and these are user-defined policies that restrict the flow of information between different profiles. Only those applications are assigned to a SP that are required to execute within that SP. And resource access for SPs is controlled by defining rules for them. Policy.db is a database of policies defined for different SPs of this security profiles application.

A. Context Detector System

Main feature of proposed system is automatic switching between security profiles based on current context that is detected by context detector system. Context detector system is responsible for detection or monitoring of activation and deactivation of defined contexts. On the detection of such event, context detector system sends a notification about this to the security profile manager.

Context is any information that can be obtained by a smartphone and that can be used to characterize the state of smartphone. And a context definition is a Boolean expression defined using any information obtained from smartphones sensors (e.g. clock : time). When context definition evaluates to be true, SP associated with that context is activated. The context_id parameter is a context identifier. Functions onTrue(context_id), onFalse(context_id) correspond to activation, deactivation of context respectively.

B. Security Profile Manager

The security profile manager has information that is linking a security profile with context. The security profile manager responsible for activation and deactivation of security profiles. The security profile manager uses following logic. If a new activated context points to the active security profile then that notification is ignored. In other cases, a security profile switch should be performed. That is the currently running security profile has to deactivate and the new security profile is active. When a security profile switch performed, security profile manager sets a command to policy decision point (PDP). To manage the SPs in user's device, GUI is provided.

C. PDP

PDP stands for Policy Decision Point. It is a fundamental point for security checks for the active SP to regulate access to resources. PDP hand over the policy check information to these managers: App manager and Rules manager.
App manager: It is responsible for deciding which apps are allowed to be executed within a security profile.
Rule manager: It is taking care of managing the rules for resource access control.

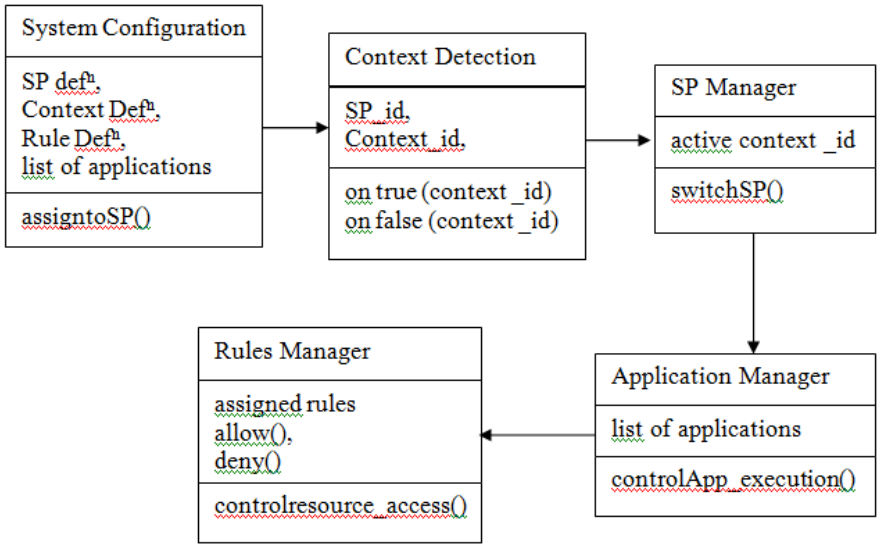

Fig. 2 Class Diagram

Class diagram shows a set of classes and their relations. Functional requirements of a system are explored using class diagram. Fig 2 shows the class diagram for proposed system.

D. Application Separation

Each SP is allocated with list of applications which are allowed to run when that profile is active. Each application during its installation receives its UID. System uses these identifiers to manage what applications can activate for every SP. During SP switching, it selects from the database, the list of applications, which are approved in activated profile. When a new SP is activated, only allowed applications for this profile will be displayed.

When new profile is activated, it may deny execution of some applications that are allowed in the previous profile. If these applications are running while the profile switch, then it is necessary to stop processes as they are no longer allowed in new security profile after the profile switch.

E. Rule Operation

Smartphones have multiple facilities like Wi-Fi, Bluetooth, mobile data etc. Access to these resources will be given to different SPs as per user's requirement. Particular SP may be restricted from accessing these resources. This type of resource access can be controlled by defining rules. Rules defined for SPs will be applied to respective security profiles as and when needed. The rules that can be assigned to SPs are: allow, deny. If rule assigned to a SP is allow, then access to the mobile resources will be permitted. And, if rule assigned to a SP is deny, then access to the mobile resources will be restricted. In this way, user can constrain unwanted use of device resources by other people by assigning rules to SPs.

V. RESULTS

Proposed system is tested taking into account various parameters like number of applications per security profile, time required to switch between security profiles, battery overhead etc. Fig. 3 and Fig. 4 show results of testing of proposed system with respect to parameters listed above.

For measuring energy overhead produced by the designed security profile application, following experiment is performed. The battery of the device is charged fully. Then, the designed application which consists of security profiles is run and for every ten

minutes, level of battery of device is measured. Three sets of this experiment are performed and average of readings is calculated. From these readings, graph for energy overhead is drawn.

Result shows that continuous running of designed application for about one hour, percentage energy overhead is about 4 percent for this application. Figure 3 shows that energy overhead is minor for designed application when compared with stock android.

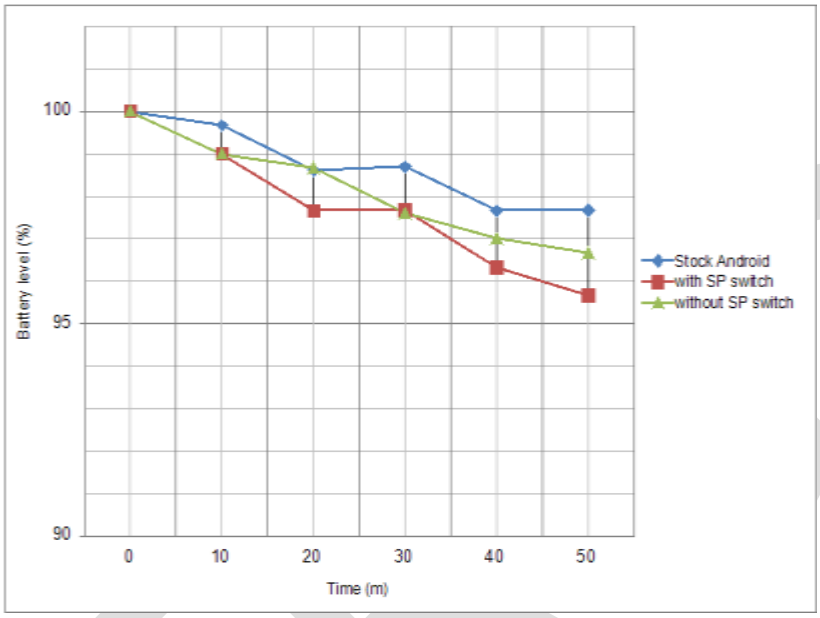

Fig. 3 Energy Overhead

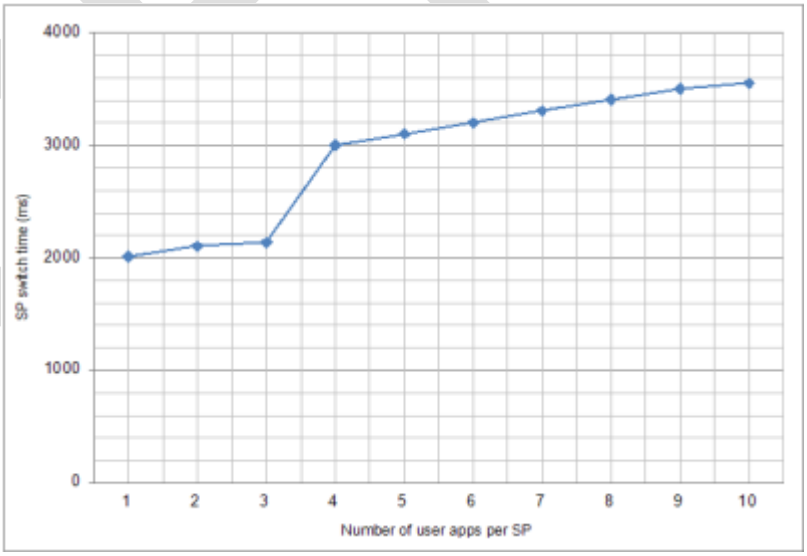

Fig. 4 Time for SP switch as a function of number of applications per SP

Here, results of the experiment measuring the time required to switch between SPs, are presented. To search the dependency between time and number of applications, the number of applications varied from 0 to 10. Three sets of this experiment are performed

and average of readings is calculated. From these readings, graph for time for SP switch is drawn. It is observed that switching time required by SP increases with increase in number of applications. It is approximately 2000 ms for 1 application to approximately 3550 ms for 10 applications per security profile. Figure 4 shows that switching time required by SP increases with increase in number of applications but this increase is very minor as this time is in msec. Hence results show that energy overhead and SP switching time, both are very less.

CONCLUSION AND FUTURE SCOPE

Smart phone security application based on separation of modes of smart phone use is developed to provide security profiles for it. Study of literature related to mobile phone security has shown drawbacks of some previous security solutions like hardcoded environments, modifications of android systems itself. Proposed system overcomes these drawbacks by providing user specified environments, application base security with data and resource access control for different kind of uses.

The application which consists of security profiles for android smart phones can have future scope in some areas. Net banking and online shopping on smart phones is one these areas. Providing such application which consists of security profiles for smart phones will make net banking and online shopping on smart phone safe, preventing misuse of personal banking information and loss. Also, child lock system can be developed using these security profiles. Also, security profiles can be developed for any type of smart phone with any type of operating system in future.

REFERENCES:

[1] M. Conti, B. Crispo, E. Fernandes, and Y. Zhauniarovich, "CR^ ePE: A System for Enforcing Fine-Grained Context-Related Policies on Android," IEEE Trans. Information Forensics and Security, vol. 7, no. 5, pp. 1426-1438, Oct. 2012.

[2] G. Russello, B. Crispo, E. Fernandes, and Y. Zhauniarovich, "YAASE: Yet Another Android Security Extension," Proc. IEEE Third Int'l Conf. Social Computing and Privacy, Security, Risk and Trust (SocialCom/PASSAT), pp. 1033-1040, 2011.

[3] D. Feth and A. Pretschner, "Flexible Data-Driven Security for Android," Proc. IEEE Sixth Int'l Conf. Software Security and Reliability (SERE '12), pp. 41-50, 2012.

[4] P.B. Kodeswaran, V. Nandakumar, S. Kapoor, P. Kamaraju, A. Joshi, and S. Mukherjea, "Securing Enterprise Data on Smartphones Using Run Time Information Flow Control," Proc. IEEE 13th Int'l Conf. Mobile Data Management (MDM '12), pp. 300-305, 2012.

[5] S. Bugiel, S. Heuser, and A.-R. Sadeghi, "Flexible and Fine- Grained Mandatory Access Control on Android for Diverse Security and Privacy Policies," Proc. 22nd USENIX Conf. Security (Security'13), 2013.

[6] J.-Y. Hwang, S.-B. Suh, S.-K. Heo, C.-J. Park, J.-M. Ryu, S.-Y. Park, and C.-R. Kim, "Xen on ARM: System Virtualization Using Xen Hypervisor for ARM-Based Secure Mobile Phones," Proc. IEEE Fifth Consumer Comm. and Networking Conf. (CCNC '08), pp. 257- 261, 2008.

[7] Anagha Parag Khedkar and Subbaraman Shaila, "Effect of Advanced Twin Operator on the performance of Genetic Algorithm", International Journal of Engineering Research and Technology, vol. 3, pp. 721-731, 2010.

[8] Anagha Parag Khedkar and Subbaraman Shaila, "The Novel Approach of Adaptive Twin Probability for Genetic Algorithm", International Journal of Advanced Studies in Computers, Science and Engineering, vol. 2, special issue 2, pp. 31-37, Sept. 2013.

[9] W. Enck, M. Ongtang, and P. McDaniel, "Understanding Android Security," IEEE Security and Privacy, vol. 7, no. 1, pp. 50-57, Jan. / Feb. 2009.

[10] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Glezer, "Google Android: A Comprehensive Security Assessment," IEEE Security and Privacy, vol. 8, no. 2, pp. 35-44, Mar./Apr. 2010.

[11] E. Yuan and J. Tong, "Attributed Based Access Control (ABAC) for Web Services," Proc. IEEE Int'l Conf. Web Services (ICWS '05), pp. 561-569, 2005.

[12] (2014) Fixmo SafeZone: Corporate Data Protection, http://fixmo.com/products/safezon.