Proactive Personalization Through Abstraction for Android Phones

Snehal S. Pundkar
Department of Computer Engineering
Smt. Kashibai Navale College of Engg.
Pune, India

P. N. Mahalle
Department of Computer Engineering
Smt. Kashibai Navale College of Engg.
Pune, India

***Abstract*— Use of smart phones is increasing day by day. Many applications are available on AppStore to facilitate the use of smart phones. Users have their personal information saved on smart phones. While downloading the application users have to allow access to personal information (e.g. contacts, coarse and fine location etc) and other facilities of the smart phones (e.g. internet, GPS, Bluetooth). But many times malicious applications which do not have access to these smart phone resources may steal the user's personal information through different attacks like intent spoofing, confuse deputy attack, permission collusion. The aim of the paper is to implement a Permission Manager (PM) model that enables us to formally define some desired security properties, which can prove a hold on Android system. The mechanism is based upon information flow control. To remain practically relevant we developed personalized Mobile Search Engine (MSE) and with the help of application we can prove that the properties hold on the android framework and we are able to secure the user's personal information. The MSE will personalize the user's web search results by considering the content and location concepts and profiling the user behavior. Goal is to develop MSE for personalizing the users search results and with the help of MSE to prove that the additionally added security properties are able to prevent malicious software from gaining access to user's personal data.**

Keywords—Android; Data Security; Personalization

I. INTRODUCTION

The goal of personalization is to deliver information that is relevant to the user. And the term proactive personalization refers to enhancing the personalization method without user intervention. It refers to studying user's behavior and automating the personalization process. In the recent years third party Applications for smart phones have become popular. In order to install the Application users are required to grant these Applications both the permission to access information on device as well as access the network. The malicious application may use network to leak information to other Applications and advertising companies or social network. For example a simple music player application may access to your location and use this information to send advertising network. Users do not have control over how their information is used by the apps and to whom it is shared. Moreover there is requirement of the mobile search engine that will rank the search results according to user's requirement. Smart phones have powerful hardware with much functionality like camera, Bluetooth, microphones, GPS and can be used via APIs. Applications take use of this APIs to perform tasks to perform convenient but privacy sensitive tasks such accessing user's phone state, call log or location information. To personalize the user Applications and secure information Android and other mobile OSs implements security mechanism such as permission system. These mechanisms in practice proved to be insufficient with increasing no of malicious Applications targeting smart phones.

This paper presents the android enforcement system in which we can specify some security properties that will ensure the security of data. To remain practically relevant we have developed personalized Mobile search engine application and prove that this application hold all the security properties.

MSE is the Mobile Search Engine which will personalize the user's search result. In order to return the highly relevant results to the user it is necessary to profile the user interest. The practical approach to capture the user's interest is by analyzing the click through data. When the query is fired for the first time it will take the results from commercial search engines and after studying the user's click-through data whenever the similar query fired next time user will get the re-ranked highly relevant result.

II. RELATED WORK

A. MSE

Objective of this paper is to provide personalization through abstraction for mobile search engines. This problem can be further divided into sub problems as follows:

- To propose a novel method for content management
- To investigate efficient method to integrate content and abstraction to provide personalization.
- To handle the security issues while providing personalization.

This paper uses the content concept and location concept to personalize the search results. For example, a person visiting India may issue the query ”hotel” and click on the search result about hotels in India. From click through MSE can learn the content preference as (room rates, facilities) and location preference as (“India”). Accordingly MSE will rerank the search results as hotels information in India. If the user is interested in particular area of India for example Noida, Delhi then the search results can further be refined by giving preference to the hotels in Noida area of Delhi.

Yokoji proposed location based system [1] requires user to manually submit the latitude longitude pair. We can profile the user's location preference in ontology based user profiles.

Most existing personalize search systems [2], [3] are based on studying the users click through data. Jaochim [3] proposed to mine document preferences through click through data. In [4] proposed to combine a spying technique to determine user preferences. Kenneth L. in [6] proposed a novel method to combine location preference and content preference to personalize the search results.

B. Enforced Security System

MockDroid [7] is a permission preference system which allows user to duplicate resources. This means system allows user to send fake information to the Applications to which they do not want to give access. For example user can give different information about the status of phone, call log or fake location details. For this it has to modify the Package Manager of the android. Package Manager store data and is the main way to share information between Applications. Data in the Package Manager is duplicated. The Application not having permission to access the information is provided with the mocked data at run time. eg. if Device ID is mocked then a random constant value is returned.

TaintDroid[8]is an information flow tracking system. It helps to track how third party Applications shares user's private information. The private stored data is labeled as 'taint'. The system monitors how third party Applications access third party Applications in real time. Sensitive information is identified as taint source. Dynamic taint analysis tracks how tainted data impacts other data in a way that may leak sensitive information.

SORBET[9] is an enforcement system that enhances the android permission system. The system can be retrofitted in the androids current architecture. Android uses the permissions which are in a string format (eg android.permission.INTERNET) to protect the components and APIs. It has included additional properties in the android permission system. The model has defined desired security properties which hold on SORBET and can be implemented on the top of android. SORBET extends Android's permission labels to make them suitable for specifying coarse-grained information-flow policies, and enforces such policies at component and application boundaries.

This paper proposes an Abstract model with several specific instantiations. Goal is to prevent software-based attacks from application level, for that we propose, an enforcement system that enables developers to use permissions to specify secrecy and integrity policies. Our solution effectively maintains runtime integrity status of application. Based on different functional behaviors of applications in android systems, we propose a set of integrity protection policies to control their interactions with others**.**

Basically, we state the properties that we wish our new mechanisms to achieve. We propose an enhanced android's permission system to support coarse-grained secrecy and integrity policies and we provide more flexible support for fine-grained and scope-limited delegation of permissions. We abstractly define access-control properties that specifies when and how the protected interface can be called and information flow properties that specify when and what information can flow to or flow from ma component. Our model investigates lower level, functional-correctness properties concerning granting and revoking permissions, since these directly affect the access-control and information flow properties.

III. PROPOSED SYSTEM

Fig. 1 shows the system architecture of the proposed system. The security of mobile devices data such as Address book, location information, online banking accounts etc has gained attention due to their increasing usage of online application in people's daily life.

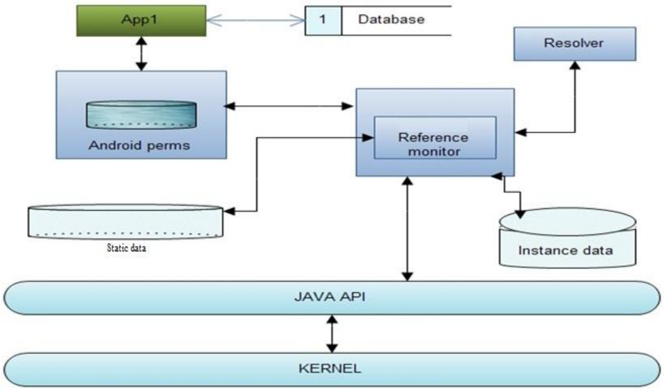

Fig. 1 System Architecture

The problem is challenging as the computing environments of these Android devices have become more open and general-purpose while at the same traditional security mechanisms.

We implement Personalized Mobile Search Engine and it adopt the meta search approach which relies on one of the commercial search engines, such as Google to perform an actual search. The client is responsible for receiving the user's requests, submitting the requests to the MSE server, displaying the returned results, and collecting his/her click through in order to derive his/her personal preferences. The MSE server, on the other hand, is responsible for handling heavy tasks such as forwarding the requests to a commercial search engine, as well as training and re-ranking of search results before they are returned to the client.

We can use MSE application to prove our enforsed security system as this application requires permission like Write SD_CARD, Location etc. First application with location permission will not show any error to access location permission and second same application without location permission will prompt us that without access application is accessing location.

Goal is to develop MSE for personalizing the users search results and with the help of MSE to prove that the additionally added security properties are able to prevent malicious software from gaining access to user's personal data.

A. Mathematical Model

1] U is main set of users
U = {u1 }
2] I is a main set of input permissions
I= {I1, I2}
3] W is the set of properties in PM
W = {w1, w2, w3, w4, w5, w6}
4] Calculate Grant and Revoke property
GRANT-TMP-T(Σ;ε,n :: grant iC_1 iC_2 P $Ƒ_{tmp}$)→(Σ'; ε)
If $\rho^{uri}{}_{\{P\}}$ (iC_1, Σ)=true where
Σ'=updateGrant(Σ,iC_1,iC_2,P,$Ƒ_{tmp}$) [9]

REVOKE(Σ;ε,n :: revoke iC_1 * P)→(Σ'; ε)
If ρp (iC_1, Σ)=true where Σ'=updateRevoke(Σ * P) [9]

5] Identify the Processes
P = {P1, P2, P3……}
1] P1 = {e1} set of processes by permission System
Where,
{e1=i|i is permission to be check on application installation.}

2] P2 = {e1, e2} Set of Processes done on permission system.
Where,
{e1=i|i set of permissions by permission system}
{e2=j|j set of properties by PM}

SpyC4.5 Method is the learns user behavior models from preferences extracted from click through data
We get (PN $\subset$ U) from SpyNB.
Po = {$po_{1,}po_2$….po_n}
U={$u_{1,}u_{2,\ldots}u_n$}
PN = {$pn_{1,}pn_{2,\ldots}pn_n$}
Identify the processes as P.
P= {Set of processes}
P = {P1, P2, P3,P4……}

If (History found about CTD) then
P1 = {e1, e2, e3, e4}
Where
{e1=i|i is to search data on selected Search Engine}
{e2=j|j is to retrieve information on search engine}
{e3=k|k is to Send CTD to RSVM for reranking as user preference}
{e4=l|l is to Check GPRS Connection on android mobile}

If (No History found about the downloading of related data) then
P1 = {e1, e2, e3}
Where
{e1=i|i is to search data on selected search engine}
{e2=j|j is to retrieve information on search engine}
{e3=l|l is to Check GPRS Connection on android mobile}

B. Algorithm

Step 1 : Let user U={ u1, u2, u3,……, un} be the users of application
Step 2 : Register as user U.
Step 3 : IF (already registered)
Login as user
Else
go to Step 2.
Step 4 : Enter the search query.
Step 5 : Click on search Button and wait for results.
Step 6 : Click on relevant websites from the results.
Step 7 : If (application is having access to any component for example GPS.
Then store the current location of user on the server database
Step 8 : If (malicious Application is not granted the GPS permission and it tries to access it)
Then the PM framework will check with the permissions and prompt the user for unauthorized access of GPS otherwise go to Step 9.
Step 9 : After your search result are obtained all this click made by user will be store on server database.
Step 10 : If user is already registered and has search results before and next time when same query is fired then re-ranking algorithm used by our application will show the most relevant results of user interest.
Step 11 : Stop.

IV. RESULTS

This paper gives the details about Personalized Mobile Search Engine. It handles the user queries on the basis of Location based queries and Content based queries. We have compared proposed system with the base paper system on the basis of time parameter. Graph analysis is based upon the time required by the algorithm to detect weather the given query is location based query or content based query and display the search result.

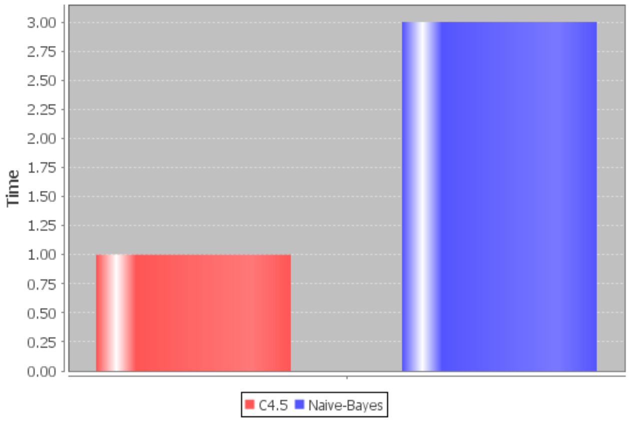

Fig.2 Total time required for execution by C4.5 v/s Naïve Bayes

V. Conclusion

This paper describes a model that enables us to formally define some desired security properties, which can prove a hold on PM. Our mechanism is based upon information flow control. Our goal is to prevent malicious software from gaining access to our personal data.

To be practically relevant we developed MSE application that will personalize the users search results. The existing systems do not take into account the content and location as two different concepts. For example, for the two different users firing query hotels in traditional search engine may receive the same search result. But one may be interested in facilities provided by the hotel like swimming pool, conference room etc and other may be interested in room rates and do not care about the facilities provided. We can use MSE application to prove our permissions system as this application requires permissions like write SD_CARD, Location etc. First application with location permission will not show any error to access location permission and second same application without location permission will prompt us that without access application is accessing location.

REFERENCES

[1] S. Yokoji, “Kokono Search: A location based search engine,” Proc. Int’l Conf. World Wide Web, 2001

[2] E. Agichtein, E. Brill, S. Dumais, R.Ragno “Learning user interaction models for predicting user websearch results preferences”, ACM SIGIR, 2006

[3] T. Joachims “Optimizing Search Engine Using Clickthrough Data”, ACM, 2002

[4] W. Ng, L. Deng, and D.L. Lee ,” “Mining user preference using spy voting for search engine personalization”, ACM, 2007

[5] World gazetteer, http://www.world-gazetteer.com/, 2012

[6] Kenneth Wai-Ting Leung, Dik Lun Lee, and Wang-Chien Lee, “PMSE: a personalized mobile search engine”, IEEE, April 2013

[7] Alastair R. Baresford, Andrew Rice, Nicolas Skehin, Ripduman Sohan, “MockDroid: trading privacy for application functionality on smartphones”, ACM,2011

[8] William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, “TaintDroid: an information flow tracking system for realtime privacy monitoring on smartphones”, ACM, 2010

[9] Elli Fragkaki,Lujo Bauer and Limin Jia”Modelling and enhancing androids permission system” ,Springer,2014

[10] Sbirlea, Burke,M.G.Pistoia “Automatic detection of inter-application permission leaks in Android applications”, IEEE, 2013