ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Security Enhancement by Remote Lock and Wipe to Personalized Smartphone Search Engine

Roly Pandey

Pune Institute of Computer Technology, University of Pune, Pune (MH) India

ABSTRACT: Android is smartphone operating system whose source code is freely available to the user it is an operating system developed by the developers of the google this operating system source code has been made freely available to the user to download make changes and experiment it is a revolutionary step in the field of the mobile operating system which has given rise to a wide market of apps providing various facilities to the customers. The idea of the project is to create personalized mobile search engine (PMSE) and

provide security for user profile by using remote lock and wipe system with integrity checking of SMS notification, PMSE that gets hold of the users preferences by the method of mining of location and the data the users' preferences by their click through data. The user preferences are organized in an ontology based , multi facet user profile , and we are providing security for user rofile if mobile lose or stolen there may be chance to hack user profile , for security purpose we can lock this mobile by sending lock command from server side application and if we get back this mobile then we can restore it by using wipe commnd , and we can use multi facet user profile for adapt a personalized filtering system which would rerank the user search result for future generation of the reranked result

KEYWORDS: Clickthrough histroy , concept, location search, mobile search engine, ontology, personalization

I. Introduction

Android is a freely available source code with security being its key feature since it s programmed with the safe language java ,especially designed for the mobile devices open , security focused mobile platform that is programmed with java . Android combines os features like efficient shared memory, preemptive multitasking , unix user identifiers (uid) and file permissions with the type safe java language and its familiar class library . The resulting security model is much more like a multiuser server than the sandbox found on the J2ME or blackberry platforms . unlike in a desktop computer environment where a user applications all run on the same UID.

The Aim of the our project of the our project is create personalized mobile search engine (PMSE) and provide security for user user profile by using remote lock and wipe system with integrity checking of SMS notification

II. PRIVACY RISKS IN ANDROID

Android poses huge privacy risks. The existing risks of the privacy in android are the risks like misappropriation , data exfiltration , misuse of personal information , and sensitive information . The existence of the advertisement these days is also a huge risk which gain access to the personal information and uses them out of users control . Prevalence of the third party ad exchange companies poses a great risk . There are libraries launched in the context of host application which leak personal information and upload personal information without the users knowledge of it.another issue being faced today is that 3rd party apps are being granted same permission as host apps . These apps generally show intrusive behavior as they collect personal information such as location contacts, mobile network location , SIM card , details , etc suspicious in nature . there are evidences where the app have breached the privacy of the user by following actions 1) collecting sms messages and 2) collecting the call log details 3) collecting camera pictures 4) collecting details of the contacts 5)collecting device phone no. 6)collecting sim card detail 7)collecting personal account details 8)prompting to install other apps 9)updating itself with new feature 9)putting ads on the notification bar 10) adding icons to the device screen 11)modifying browser bookmark 12)Playing audio ad after dialing 13)displaying ad in sms box 14)changing the browser homepage 15)sending an sms when clicking on ads 16)collecting recorded audio1 clips 17) collecting calendar event details . In todays android market the paid and the unpaid apps have got no difference when it comes to the privacy both are equally vulnerable towards privacy breach .one of the very common concern or security risk of the android is the vulnerability of the data present . if the data is vulnerable and if suppose the android phone gets lost or stolen . what is so particular in android in regard to the security is that it poses a major risk because of its lack of hardware data encryption in such a scenario stored data can be protected by a remote lock/wipe of the data

III. SECURITY RISKS

There are various types of security risks that android poses in a recent study of the US government . Android being an open source platform it is quite susceptible to malware attacks. Android is susceptible to huge amount of malware threats which generally affect the smartphones . Sms text represent a large part of it , there is a commom issue where the rootkit are installed on million of devices These days the active cyber criminals sometimes create fake google play domain which misleads the user in downloading malicious type of apps, loss of device is major topic of worry since a large no of smartphone usetrs lose their data and what is particular in android is that they are managed via the desktop sync unlike the apple iphone in which all the data lost can be recovered from itunes Presense of the unsubstatntial and inadequate password . lack of hardware encryption is another major issue in the android os and it this is where the idea of having remote lock/wipe comes into the picture and proofs to be a very useful concept. Smsing is another type of security risk where the smartphone is made to sent sms to malicious link is costing the user of the smartphone huge bills that that he has to pay without any awareness of what actually goes within.

IV.THREATS IN ANDROID

There are several threats facing the android system and the following sections will list and explain some of the more common threats . A single malicious application can represent more than one of these threats Trojans-Trojan is a malicious piece of code which contains harmful data which gets hold of the users computer and infects the file stored in the users pc .it does serious harm and damages.it spreads even more as it progresses.

Spyware : Spyware are infected harmful viruses or piece of code their main purpose is to siphon off the private and confidential information from the users device and to leak to out to a third party website . spywares on most occasions are manually implanted on a users phone to let it siphon off the valuable information and the data off the users phone to a third party.

Root Exploits : Root exploits are created by the very own members of the android community for gaining super rights to the device for becoming a supersuser

Botnet : botnet is a network of already insecure devices which generally an attacker uses to for his ow selfish motive to send the data outside the computer as part of the denial of service attack

Premium sms sender : There are present some malicious applications in the android market , these suspicious apps ask for users permission to send messages and send messages from the users phone at premium rate numbers costing them huge amount of money without their awareness

Drive by download : drive by download is a type of attack where the user is prompted to download some content which may be presented to the user as a system update or improved version so when user tries to download it it leads the user to visit a insecure website and the user computer gets infected by trojan

Proof of Concept : Proof of concept Trojan are usually the lowest dangerous type of virus they are usually there just to show a vulnerability or just to brag right they usually do not have or carry any potential threat in them

Destructive Trojans : Destructive Trojans are different from the Trojan in a way that they usually destroy files from user computers or make them infected or corrupt it is usually result in file corruption and phone wiping.

Phishing : the android market these days is flooded with phishing apps which pretend to be real and after users use it to login it transmits that information to a third party website

Capability Leaking : it is done by malicious application which leaks priviliges to other applications which do not have that sort of privilege .Information Leaking : this type of attack leaks sensitive information to other applications present on the device

IV. EXISTING SYSTEM

In mobile search the interactions between the user and search engine are limited by small form factors of mobile devices also search engine does not think personally , it gives the results globally which are same for all the users and existing system not says about the security of the mobile if the mobile lost or stolen

V. PROPOSED SYSTEM

We propose a personalized mobile search engine PMSE that captures that users preferences in the form of concepts by mining their clickthrough data The user preferences are organized in an ontology based multifacet user profile and we are providing security for user profile if mobile lost or stolen there is a risk of user profile getting hacked for security purpose we can lock this mobile by sending lock command from the server side application and if we will get back this mobile than we can restrore it by using wipe command and we can use multi facet user profile to adapt a personalized ranking function for rank adaptation of future search results

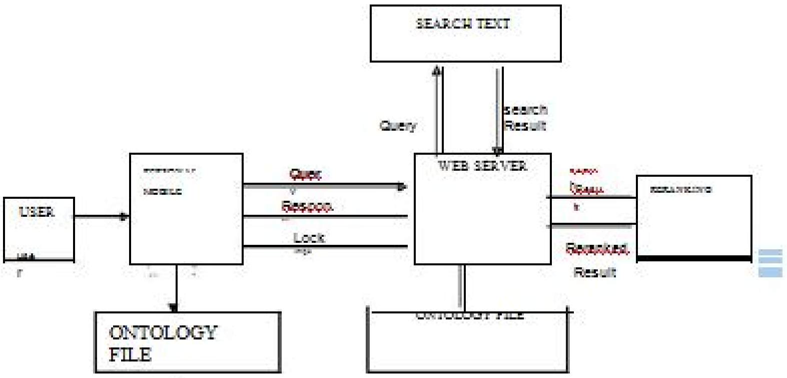

Fig 1 SYSTEM ARCHITECTURE

VI. RELATED WORK

Clickthrough history has ben made use of in the determination of the users liking and choices and the it is made use to henceforth reflect it on the search result. Joachims [3] proposed to use data mining as the method to determine search result which are refine and reranked using clickthrough data .Ng [7] made a proposition where he suggested to get together a spying method with a use of a predictable model to predict the user liking and preferences for the future search results leung [2] came up with a method to give predictions regarding the user conceptual choices from taking help from the clickthrough history for various criteria to personalize the queries.

VII. MATHEMATICS

Let Q = input is given as user query to PMSE server

Q = { HI,PS,NS }

Where

HI is history which maintained in history of search

PS is previous search information which maintains clickthrough history

NS is new search result which comes by using previous search result + New Result

S is set of search engine S = {s1,s2, s3,s4,……sn}
Identify the searching on servers

Q={q1,q2,q3,q4,…..qn}

Where Q is main set of searching query on server q1,q2,q3,q4……..qn
q = {HI,CTD,NS,RSVM…..}

RSVM

RSVM = Receive the extracted data on RSVM server which sre

send through android mobile

NS = new search result which come by previous search result+new result

Spy NB Method is the learns user behavior models from

preferences extracted from clickthrough data

Spy NB = {Po,U,PN}
Let Po be the positive set
U the unlabeled set
PN the predicted negative set
We get (PN (U) from Spy NB
Po = {Po1,Po2,….,Pon}
U = {u1,u2,….,un}
PN={pn1,pn2,…..,pnn}

P={set of processes}

P={P1,P2,P3,P4…..}

If (History found about CTD) then P1={e1,e2,e3,e4}
Where

{e1=i|j is to search data 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 references }

{e4=l|l is to check GPRS connection on android mobile }

If (No History found about the downloading of the related data)

Then

P1 = {e1,e2,e4} Where

{e1 = i|j is to search data on selected search engine} {e2 = j|j is to retrieve information on search engine} {e4= l|l is to check gprs connection on android mobile }

Overall subsets used in application A = {S,HI,P,PS,NS,Q}
Initial condition as Io

a) Android device should be activated the gprs connection b)Admin have good internet connection

VIII. CONCLUSION

The system proposes the mechanism to provide security to theuser by using remote ock/wipe which protects the users data to prevent the suspicious users from leaking users personal data and information and launching attacks on the phone

REFERENCES

[1] android-apktool:Tool for reengineering Android apk files http://code.google.com/p/android-apktool/
[2] Kenneth wai-ting leung and dik lun lee and wang chien lee"A personalized mobile search engine", IEEE Trans. Knowlwdge and data engineering vol 25 , no 4, 2013
[3] T joachims , "optimizing search engines using clickthrough data" Proc ACM SIGKDD Int'l conf. knowledge discovery and data mining,2002
[4] Q Gan J Attenberg A Markowetz and T suel "analysis of geographic queries in a search log" Proc. First int'l workshop location and the web (locweb),2008
[5] S Yokoji, "kokono search : A location based search engine ," Proc . Int'l conf. World Wide Web (www), 2001
[6] Y-Y chen T suel, and A markowetz "efficient query Processing in geographic web search engines" Proc int'l ACM SIGIR cont research and development in information retrieval(SIGIR) 2006
[7] W.Ng , L.Deng, and D L Lee "Mining user preference using Spy Voting for search engine personalization", ACM Trans. Internet Technology , vol 7, no. 4 , article 19 , 2007
.