Biohouse, Volume 1: Issue 1, May-June 2015

Biohouse Journal of Computer Science

ISSN 2379-1500

Multi Layered Approach for Privacy Preservation in Smart Devices

G Kiran Kumar, Professor
CSE Department, MLR Institute of Technology,
Hyderabad, INDIA
hodcse@mlrinstitutions.ac.in
mobile: +91-9160404642

P Ram Mohan Rao, Associate Professor
CSE Department, MLR Institute of Technology,
Hyderabad, INDIA
rammohanrao@mlrinstitutions.ac.in
mobile: +91-9959638850

Abstract: *In today's Information and Communication Technologies (ICT) backdrop, privacy of users information is the most important and desired feature. However émergence of Smart devices like tablets, ipads and smart phones have seen significant increase in the user base of ICT. In this paper a study has been made on ANDROID operating system's security vulnerabilities and proposed most compelling changes to be incorporated in the operating system to ensure privacy preservation in smart devices*

Keywords: *Privacy, User Interface Design, Android, Permissions, Android OS*

I. Introduction

Privacy is the ability of individuals to control the terms under which their personal information is shared or accessed. Today human's life relies on Information and Communication Technologies (ICT) in the form of Social networking, communication with friends and colleagues, E-Commerce, Banking, Retail etc. Larger part of the society is now dependent on the ICT[1]. It is very clear that the users of ICT need not be computer professionals and privacy becomes hard to understand for these users and also every user expects ease of use. To understand the essence of usable privacy, let us consider the following example.

Almost each and every smart phone user would have installed whatsapp. Many users are not aware of the permissions which the app demands to get installed. Even if the app displays the list of permissions required users show least interest in reading them. Not only whatsapp many other apps can access lots of our personal information including contacts, photos, videos etc. Apart from the ignorance of users there are so many vulnerabilities in the operating system itself which can compromise the privacy of the smart phone user. We have taken ANDROID as case study since ANDROID is most widely used smart phone platform.

Major Challenges in Privacy Preservation

1. ANDROID Architecture itself has got some serious vulnerability. The ANDROID OS uses Linux kernel which is open source and encourages lot of customization which is not good from the privacy preservation point of view.

2. ANDROID OS implementations are not common across all vendors. There will vendor specific features in ANDROID Devices

3. There is no guarantee that an app downloaded from Google store is safe and does not contain any malware. Google's Bouncer may filter apps containing malware but still it is not enough. Malware can be inserted into the app during upgrades and additions of patches provided from the vendor's site. This app when shared will also propagate the underlying malware. [6]

4. Lack of awareness among users is also a major issue. Many users don't even know that an app can access personal information.

5. Deleting files from the smart phone does not really delete the files. It will simply make changes to the file entry in the file table. Selling a smart phone may imply selling your identity and confidential private information

.

II. Related Work

It has been observed that people are not privacy sensible. People share lot of personal information in social networking sites, perform lot of financial transactions like net banking, booking movie tickets etc through smart phone. Many apps do not even show the list of permissions required and user simply accepts the license agreement and installs the app. Users are not aware of what information an app can steal from the phone.

Typical Permissions in any ANDROID OS include

1. *Network Access*
2. *Access to call log*
3. *Access to internal storage*
4. *Access to external storage*
5. *Access to contacts and media*

Very common type of access that gaming apps use are location tracking and sharing [2] [3] . Most often the users are not aware of it. Many apps do not give proper notifications about the permissions. If some apps request some types of permissions the users may misinterpret them. For example SEND_SMS request is made by an app, the user may think that this app will allow him to send SMS messages[4]. But the fact is the app is requesting to access text messages and in turn forward them to the app developer.

The current system is a manual one where in the department maintains all the information in the form of records and paper work. There by collecting necessary information with require a

manual search in the records. Selection of a faculty member for a job is done by manually by HOD approaching the staff and confirming the availability of the staff. Transfer of information between different people in the department is in the form of documents.

The existing system suffers various problems

- Preparation of information in department is in the form of documents taking more time and manpower.
- Due to mismanagement and communication gaps, the work is delayed to later date than the due date.
- Unavailability of proper information to different levels of faculties within the department.

III. EXISTING SYSTEM

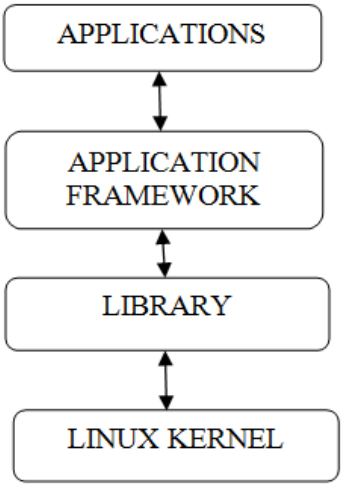

Fig.1 Existing Architecture of ANDROID

ANDROID OS is built using Linux kernel 2.6 and the library framework consists of core libraries and Dalvik Virtual Machine. Application framework contains various activity managers for the applications to interact. There is a need for a special security layer to address above discussed challenges which is our proposed work which in not found in Fig.1

One of the most common threat is phishing because many users can't even differentiate url's properly and can land in to fake websites contributing to information leakage

Ex: www.facebook.com/3456.php

In the above link many users assume it to be a link to facebook where as the alphabet 'c' in the above url is not English alphabet it is a Unicode character. Smart phone users need to be educated in this direction.

IV. PROPOSED SYSTEM

A multi layered approach to enhance and strengthen existing ANDROID OS is needed following is the layer to be added as shown in the Fig 2.The new security layer acts as an interface between the application framework and the core libraries. It is highly recommended that the ANDROID distributions across all vendors should be same.

Key Points to be followed are

- No Vendor should access the layers below security layer ensuring no customization of ROM
- Preferably the LINUX Kernel should be replaced with UNIX or any other OS which is not open source.

The security layer should monitor the downloads, installations and usage of apps in the smart phone.

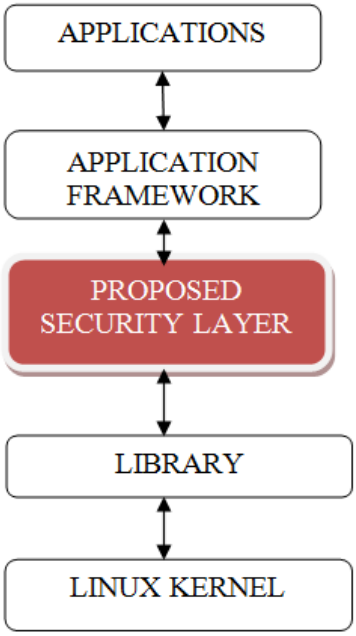

Fig 2. Proposed security layer in ANDROID OS

The proposed security layer should contain three components

- Application Sniffer
- Malware detector
- Sophisticated File system manager

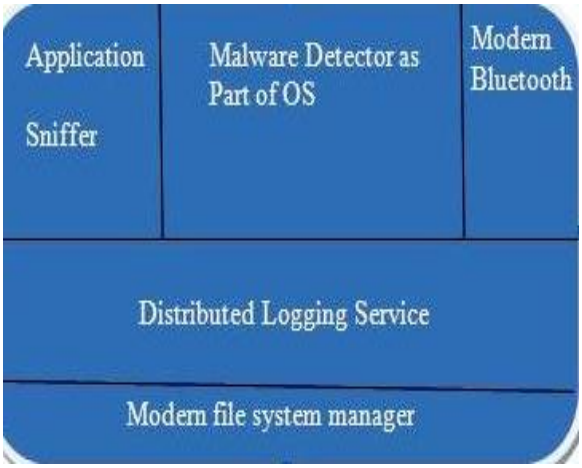

Fig 3. Components of Proposed Security Layer

Each component of Proposed Security layer(Fig 3) are discussed below.

International Journal Series

ISSN 2379-1500

Application Sniffer:

Any app should run in a separate sandbox with unique id and should not share any information with other apps which are running. Total sandboxing and isolation must be ensured. Application sniffer should make sure the above said property. Application sniffer must also check for any privilege escalation attempts made by an app and block such attempts.

Malware Detector:

Any app downloaded from Google Play store will not contain any malware because Bouncer is a special program of Google which will not allow any suspicious app to be loaded into Store. But malware will infect the device when we start downloading patches or updates from the respective sites. There are so many malware detector apps available but one cannot trust these apps also since they can also steal private information. Sharing the app will also create the similar effect. So malware detector should be part of the OS itself.

Google Patches:

If Google has identified any bug in the ANDOID OS they will release a patch to that bug. These patches are implemented separately by the vendors. Every vendor should use the same patch without customization. It is highly recommended that the update should be directly installed into android device via install_asset command

Deleting Files:

ANDROID file system is also an interesting aspect of privacy. If we delete a file from the smart phone it does not really remove that file rather it will make changes to the file entry. If we sell our smart phone it may also lead to leakage of our private and confidential information. It is again recommended that once a file is deleted it should be really erased from the memory for the sake of privacy and security.

Rooting is one of the major issue in present ANDROID versions. Rooting should be disabled in ANDROID OS. Rooting is the process in which the limitations are removed and full-access is allowed. Once rooted, the Android phone owner will have more control over many settings, features and performance of their phone.

The security layer should ensure logging service to run in sandboxed environment. Many apps tend to write status messages to the logging service containing parameters which disclose personal details of their device owners. For example, several GPS-based apps were found to write the device's geo-coordinates to the logging service in regular intervals, thus providing full profiles on the device owner's movements to other apps installed. Thus the security layer should ensure that the logging service should be decentralized.

It is a typical feature of malware to connect infected machines for forming botnets which are useful to their operators for various reasons. Typical botnet functionality includes spam message delivery, stealing credentials Spam message delivery and obtaining credentials is significantly simplified on smartphones with privileged access by an adversary. Any credentials for communication applications can be stolen, once root privileges are acquired . This way, smartphones can not only serve as spam relays themselves, but provide spammers with high quality contact details from various services' address books. Alternatively, spammers can use stolen credentials to deliver spam messages from other machines with better network capacity.

Some of the other attack vectors are Bluetooth and Wifi connections. Both of them are vulnerable to man in middle attacks. So the new security layer should ensure more sophisticated protocols for Bluetooth and wifi..It is even possible to spread malware via Bluetooth.

1. Need to provide additional security layer with following features.

2. User Interface Design should be carried out by considering all security and privacy attributes. User Interface Designers, Security Professionals and Psychology experts should work together in providing a user friendly application simultaneously providing privacy controls to the user. This is a new area of research which enables Usable Privacy.

3. Creating Awareness among Users: It is immediate requirement to spread awareness among the users of smart phones regarding the data leak that can occur due to improper handling of the apps. Users should realize that they are carrying Hacker in their pocket.

4. Notifications: Many apps do not give proper notifications regarding the resources they are going to access. It should be made mandatory that an app should provide complete list of permissions and resources it demands. Even users should not be able to skip reading the license agreements. Every user should read the license agreement.

5. Universal Standards: All Mobile Operating Systems should provide a standard API interface for the app developers by considering all possible security attributes.

6. Apps should not leave any kind of traces and more specifically net banking, online shopping apps data should be erased automatically.

V. CONCLUSIONS

The existing ANDROID OS has lot of security vulnerabilities like centralized logging service, customizable ROM, Rooting etc. Which leads to leakage of private information. With the proposed security layer containing Application sniffer, Malware detector, Modern Bluetooth, Distributed Logging Service and Modern File System manager can ensure privacy preservation to the maximum extent in Smart Phones.

ISSN 2379-1500

VI. REFERENCES

[1] M. Hettig, E. Kiss, J.-F. Kassel, S. Weber, M. Harbach, Visualizing Risk by Example: Demonstrating Threats Arising From Android Apps, *M. Smith Symposium on Usable Privacy and Security (SOUPS), Newcastle, UK*, July 24–26, 2013,

[2] L. Barkhuus and A. Dey. Location-based services for mobile telephony: a study of users' privacy concerns, *Proceedings of the International Conference on Human-Computer Interaction*, 2003.

[3] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. A Survey of Mobile Malware in the Wild, *Proceedings of the ACM Workshop on Security and Privacy in Mobile Devices (SPSM)*, 2011.

[4] A. P. Felt, K. Greenwood, and D. Wagner. The Effectiveness of Application Permissions, *Proceedings of the USENIX Conference on Web Application Development (WebApps)*, 2011.

[5] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, David Wagner University of California, Berkeley, Android Permissions Demystified, *CCS'11, Chicago, Illinois, USA. Copyright 2011 ACM 978-1-4503-0948-6/11/10 ...$10.00,* October 17–21, 2011

[6] *Android OS Security: Risks and Limitations*

Short Biodata for the Authors

Mr. G Kiran Kumar is working as Head of Department Computer Science Engineering and his research interests are Algorithms, Networks, Mobile Computing Big Data and Cloud Computing. He has got 14 years of teaching experience

Mr. Ram Mohan Rao working as Associate Professor in Department of Computer Science and Engineering has 10 years of teaching experience and his research interest are web application security and usable privacy

ISSN 2379-1500