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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

# A Survey on Runtime Information Gathering System

Srijit Nair[1], Akshay Damodaran[1], Hrishikesh Balakrishnan[1], Prof. Namita Pulgam[2]

B.E. Students, Dept. of Computer Science, Ramrao Adik Institute of Technology, Mumbai, India[1]

Assistant Professor, Dept. of Computer Science, Ramrao Adik Institute of Technology, Mumbai, India[2]

**ABSTRACT**: Stealing of information by apps is always considered to be one of the most critical threats to Android security. Though Android has permission model to allow/deny access to certain resources but that is a broader permission. In order to conclude that an App is malicious, gathering of information like its name, path, memory usage, CPU usage and network information that it creates is important. Also advanced information like is it scheduling itself or not, etc. is also required to be known. So we are proposing Runtime Information Gathering System (RIGS). RIGS main aim is to monitor network access of the application and apply data and functionality restrictions. Other concern is handling the data leaks of a particular organization over numerous devices working under that organization's network. RIGS run the device on private network under firewall restrictions thus creating a clean baseline for android security. Runtime information gathering system allows the organization to monitor the data movement between these devices in turn reducing the chances of a major information leak. RIGS allow monitoring the behaviour of a particular application for a period of time before concluding whether the application is malicious or not.

**KEYWORDS**: RIGS, Android System

## I. INTRODUCTION

Android's unrestricted and open source application market have made it a popular platform for security threats. Access to privacy and security relevant parts of Android's rich API is controlled by an application permission system during installation. Each application must declare upfront what permissions it requires, and the user is notified during installation about what permissions it will receive. If a user does not want to grant permission to an application, he or she can cancel the installation process. Install-time permissions can provide users with control over their privacy and reduce the impact of bugs in system. However, an install-time permission system is ineffective if developers routinely request more permissions than they require. Applications with extra system functionality access expose users to unnecessary permission warnings which increase the impact of any attacks or bugs. Run time information gathering aims to monitor network access of the application and apply data and functionality restrictions thus making it configurable as per the needs of organization. It tracks the name, path, memory usage, CPU usage and network sockets that these applications creates. Analysing these parameters would decide whether an app is malicious or not. RIGS gives the facility to block those apps and flag them.

## II. RELATED WORK

Android applications have been limited in their understanding of permission usage. Only method of security check is reading the permission requirements during installation and checking them against a set of security rules. [1] Due to the lack of a common definition for security and the sheer volume of applications ensure some malicious, questionable, and vulnerable applications to find their way to market. [6] Attackers insert a malware in an app and distribute it to common users through the open market or internet targeting common smart devices equipped with the Android platform. [11] .The android market has no security scans over the applications being uploaded on its market. Some apps

DOI: 10.15680/IJIRCCE.2017. 0504196

can exploit the services of another app without permission request. [7] To track a application’s behaviour, it is a must to collect and analyse several events and attribute to a single originating entity, in order to gain information relating to the originating entity.[2] Online social application gives data that contains user’s precise location, his gender or name, and even subject’s unique social networking identifier. The combination of all this information provides a tool to accurately profile users. The necessary idea is that users must also be able to choose what data is collected about them. [3] They must keep the right to access, modify and delete them. Most sites provide coarse-grained privacy controls but majority of users do not use this feature because they find it too complex. [4] Understanding of what portion of it really needs to be accessed by applications needs to be developed. [5] Most organizations store large amounts of user related and company data. Security breaches can result in the disclosure of critical information or the loss of a capability that can affect the entire organization. [8] Inadequate management of user authority and acquisition of authority to share userID can act as a weakness of android operating system. [9] Intercepting the mobile application’s API call during run time can catch majority of malicious behaviours but it requires changing the android API. [10] VPN is a better choice for providing network security as it realizes a private network for use within any public network. [12]

## III. PROPOSED METHODOLOGY

Major concern regarding android security is a genuine application behaving as a malicious app. This is due user’s lack of awareness and control over an application’s access. RIGS main aim is to monitor network access of the application and apply data and functionality restrictions .Other concern is handling the data leaks of a particular organization over numerous devices working under that organization’s network. RIGS run the device on private network under firewall restrictions thus creating a clean baseline for android security. Runtime information gathering system allows the organization to monitor the data movement between these devices in turn reducing the chances of a major information leak. RIGS allow monitoring the behaviour of a particular application for a period of time before concluding whether the application is malicious or not. The system after careful analysis has been identified to be presented with the following modules:

- Information Gathering Module
- Communication Agent
- UI Module.
- Action Module
- Parameter Information Collection Module
- Anomaly Detection module

### User Interface Module

The user interface module id the android application displayed to the user. This module provides three options to the user.

Recent Info: This option displays user with the most recent scan information which was already stored in the database.
Live Info: Performs a live scan at that instant and displays it to user and also appends into database.
History: Displays list of all the scanned reports to the user and user can view through them.

### Communication Agent

Communication agent communicates with all the modules in the application layer and transfers the information between them. Any communication or data transfer has to be performed using communication agent only.

### Action Module

The action module allows the user to either restrict or uninstall the app depending on the level of security intrusion. It allows the system administrator to restrict network access to certain applications. It can also stop certain functionalities.

### Anomaly Detection Module

This module decides which application is malicious analyzing the information gathered by the information gathering module.

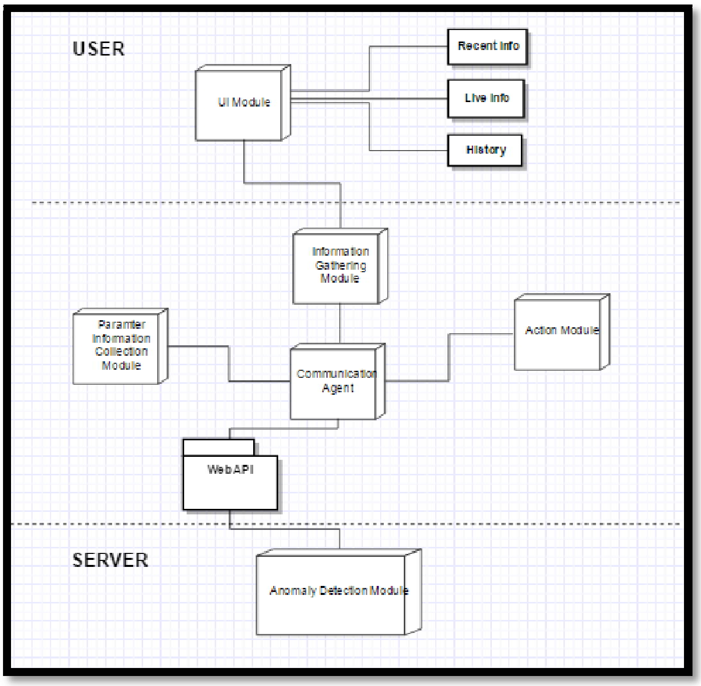

Fig 1: Overall System Design

## IV. Android Application

We have implemented this entire system in an android application as front end and back end database on phpmyAdmin. This system works with any android device on which it is installed. RIGS system has two different user categories i.e. Standard user and Administrator. A user logged in with standard user account can view his device's system details collected by RIGS. An administrator can restrict application functionalities and activate/deactivate the information collection module. Once the information collection module is activated it keeps sending information in every 10 sec interval to be stored in database for any further analysing. We use json packages to send data from user's device to main database.

## V. Conclusion

Runtime Information gathering system is a monitoring system that analyses your android device scanning and gathering information which can be used in detecting malicious application. The advantage of the system will be providing the user and the organization a better understanding of the application running on their device thus improving the security over it. The system will allow the user to restrict access to certain application which it considers as malicious. The administrators can handle all the profile generation and restriction of functionalities before circulating the devices in organization.

## VI. Future Work

Future work on this system can be addition of new functionalities like Behavioral and Pattern analysis module for detection of anomalies. Over the period few months, the data collected through information gathering module is used understand the behavior and patterns of a particular application thus creating a system which can restrict or evoke permissions on its own. Introduction of compatible software for employee’s personal devices instead of providing a customized device will be useful. In future RIGS application will be made as a device owner application, at organizations where mobile usage is restricted. .This will allow organizations to permit personal android devices instead of customized device.

## REFERENCES

1. Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, David Wagner,’ Android Permissions Demystified’, 11th Computer Security Conference, pp. 627-638,2012.
2. Mireille Hildebrandt,’ Profiling: From Data to Knowledge,’ 30thDatenschutz und Datensicherheit, pp.548-552, 2006.
3. Balachander Krishnamurthy, Craig E. Wills’, Privacy leakage in mobile online social networks,’ Workshop on Online Social Networks USENIX Association Berkeley, 2010.
4. Evelyne Beatrix Cleff,’ Privacy issues in mobile advertising,’ International Review of Law, Computers and Technology - Cyberspace: Who's (Should be) the King of the Castle?, 2007
5. Information revelation and privacy in online social networks,’ Ralph Gross, Alessandro Acquist,’5th Computer Security Conference,pp.71-80 ,2005
6. William Enck, Damien Octeau, Patrick McDaniel, and Swarat Chaudhuri,’ A Study of Android Application Security.’ SEC'11 Proceedings of the 20th USENIX conference on Security, pp. 21-21, 2011.
7. Tiwari Mohini, Srivastava Ashish Kumar and Gupta Nitesh,’ Review on Android and Smartphone Security,’ Research Journal of Computer and Information Technology Sciences, Vol.1 (6), pp.12-19, 2013.
8. Kamal Shah and Tanvi Kapdi,’ Disclosing Malicious Traffic For Network Security.’International Journal of Advances in Engineering & Technology, Vol. 7 Issue 6, pp. 1701-1706, 2015.
9. Jae-Kyung Park and Sang-Yong Choi,’ Studying Security Weaknesses of Android System,’ International Journal of Security and Its Applications, Vol. 9 Issue 3, pp. 7-12, 2015.
10. Mingshen Sun, Min Zheng, John C.S. Lui, Xuxian Jiang,’ Design and Implementation of an Android Host-based Intrusion Prevention System, CUHK, 2014.
11. You Joung Ham, Daeyeol Moon, Hyung-Woo Lee, Jae Deok Lim and Jeong Nyeo Kim,’ Android Mobile Application stem Call Event Pattern Analysis for Determination of Malicious Attack,’ International Journal of Security and Its Applications, Vol.8 Issue 1,pp. 231-246, 2014.
12. Xingkui Wang and Xinguang Peng,’ VPN Gateway Research in Wireless Network Based on SSL Technology,’ International Journal of u-and e-Service, Science and Technology Vol. 8 Issue 4, pp.17-26, 2015.

## BIOGRAPHY

**Srijit Nair, Akshay Damodaran, Hrishikesh Balakrishnan** are students of B.E Computer Science Department, R.A.I.T Nerul, Mumbai, India

**Prof. Namita Pulgam** is Assistant Professor in Computer Science Department, R.A.I.T Nerul, Mumbai, India

DOI: 10.15680/IJIRCCE.2017. 0504196