IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13362

APP SECURITY ANALYSER: AI BASED FRAUD DETECTION USING SENTIMENT INSIGHT

SIVASAMY P[1], DR. J. SAVITHA[2]

Department of Information Technology, Dr.N.G.P. Arts and Science College, Coimbatore, Tamilnadu, India[1]

Professor, Department of Information, Technology, Dr.N.G.P. Arts and Science College, Coimbatore, Tamilnadu, India[2]

Abstract: Mobile App store ranking fraud is given the meaning that it refers to deceptive or malicious acts that perform the function of promoting the Apps in the popular list. Really, it grows more and more usual for developers of Apps to use dishonest actions, such as overstating sales of their Apps or providing untrue App ratings, to commit ranking fraud. While the importance of ranking fraud prevention has been comprehensively understood, research and knowledge on this front are limited. In this regard, in this paper, we discuss a thorough overview of ranking fraud and propose a ranking fraud detection system for mobile Apps. Specifically, we first propose to accurately identify the ranking fraud by mining active time, i.e., leading sessions, of mobile Apps. Such trailblazing sessions may be used for local anomaly identification instead of global anomaly of App rankings. Besides, we investigate three evidences, i.e., ranking based evidences, rating based evidences and review based evidences, by explaining Apps' ranking, rating and review behaviors through statistical hypotheses tests.

I. INTRODUCTION

Smart phones are trendier than ever before. Part of the reason that this is true is the fact that the Google Android operating system (OS) is a platform that enables programmers to create programs and release them for free within an open market. According to the most recent analyzes, more than one billion Android devices have been activated with a staggering rate of growth at 1.4 million devices per day. With such growth, it is completely imperative that developers understand how to build secure Android apps. With increasing numbers of applications available out there for Android; spyware is becoming a biggest concern. Various malicious applications, from clone banking applications to an SMS Trojan inside a clone media player tools, have been discovered on the Android Market since the year. However, there are other forms of malware that might also come into being. What about using the disguise of a well-known application? For example, think of an application talking to be the latest version of a well-known Twitter client, in reality pushing spyware in the background and forwarding all personal data to the attacker.

II. EXISTING SYSTEM

Here a software framework is established in this system that maintains application security by re-writing the application's byte-code according to the user's requirement. The static analysis technique is applied by this system and decides the methods that are to be altered based on the data supplied by the user. The constructed methods substitute the altered methods, and these altered methods are called. The experiment was conducted on 30 randomly chosen applications randomly picked from 100 top-selling applications from the Android Market. The system overloads the primitive methods, i.e., Math.sqrt, url.OpenStream, and StringBuilder.append, and re-replaces them with custom methods. In addition, the authors incorporated logging facilities into the system and tested the methods directly to verify whether they were indeed called or not. According to their results, they encountered no issues rewriting the application, and it ran correctly without any bugs.

EXISTING SYSTEM

In this system, a software framework is developed that ensures application security by recompiling the byte-code of the application based on the user's requirement. The system uses the static analysis method and identifies the methods to be modified based on the information provided by the user. The methods developed replace the modified methods, and the modified methods are invoked. The experiment was performed on 30 rando Here, we have a closer look at permissions users grant to applications on Android, a popular mobile operating system for smart phones. Interestingly, Android does

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13362

not impose sufficient control to their users regarding what applications are allowed to do. We offer tracking and monitoring of the malicious activity of the apps the user has installed even from playstore using trusted permission based security model. We demonstrate the feasibility of a permission tracking feature, but say that significant modifications to Android itself will be needed in order to provide satisfactory control over apps' permissions and users' privacy. m apps randomly selected from 100 best-selling apps of the Android Market. The system traps the low-level calls, i.e., Math.sqrt, url.OpenStream, and StringBuilder.append, and re-replaces them with special calls. In addition, the authors added logging features into the system and checked the calls directly to observe whether they were actually called or not. As per their experience, they did not encounter any problems rewriting the application, and it executed properly without any glitches.

ADVANTAGES OF PROPOSED SYSTEM

The significant benefits of the E-Assignment are

- Having the capability to create security policies.
- Automatically identifies the loss of confidential information
- The tool created tracks data flow through applications and takes security actions.
- No loss of data

ADVANTAGES OF E- ASSIGNMENT SYSTEM

The major advantages of the E-Assignment are

- \tSecurity policies can be created.
- \tIt detects leakage of sensitive information automatically
- \tThe tool captures the data flow in applications and enforces security controls.
- \tLoss of no data

III. SYSTEM DESIGN AND IMPLEMENTATION

FILE DESIGN

In computing, a file design (or filesystem) is used to control how data is stored and fetched. Without a file system, information placed in a storage location would be one enormous clump of information with no way of knowing where the one piece of information ends and another begins. By partitioning the information into sections, and labeling each section, the information can be separated and designated so that it can be easily identified. Labeled after the process by which paper-based information systems are identified, each group of data is a "file". The arrangement and rules of logic used to manage the sets of information and their identifiers are known as a "file system".

Certain file systems are hosted on local storage devices; others provide file access over a network protocol. There are "virtual" file systems, in which the "files" available are computed on demand or a mapping into a second file system acting as backing store. File system manages access to files' data and data about files. It is responsible for managing space arrangement; dependability, effectiveness, and optimizing regarding the lower storage medium is a major design consideration.

Input Design

Input design is all about making sure that data entered by users into a computer system is accurate, logical, and easy to process. The goal is to ensure that data entry is smooth and free from errors, as these errors can affect the system's performance and the integrity of the information stored.

The main objectives of input design are

- Collecting data from the source
- Transferring data into an input form
- Converting that data into a format the computer can understand
- Verifying the converted data
- Checking for accuracy
- Sending the data to the computer
- Validating the input data
- Ensuring thorough data collection to prevent errors

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13362

Types of Input

- Internal Input: This refers to when users directly interact with the system.
- Operational Input: The computer department or system administrators communicate with the system.
- Computerized Input: Inputs come from other internal or external systems in a digital format.
- Interactive Input: Users input data during an interaction or conversation with the system.

Key Considerations in Input Design

Nature of Input Processing: How the system handles and processes the data entered.
Flexibility and Validation Rules: The system should be adaptable and have thorough checks in place to validate the entered data.
Priority Handling: The system should manage input procedures based on priority levels.
System Integration: The input design should be compatible with other parts of the system.
Form Design: The design of input forms should make data entry accurate and efficient.
File Relationships: Ensuring that the input data aligns with other files and data storage systems.

Output Design

Output design is all about the results and information that a system generates for its users. It's the reason the system exists in the first place, and it's what ultimately determines how valuable the system is. The effectiveness of the system is judged by the quality and usefulness of the output it provides.

The goals of the system are realized through its output. By understanding what the system is meant to achieve, we can figure out the kinds of outputs needed. These outputs can come in different forms, such as reports, screen displays, printed forms, or even graphs and images.

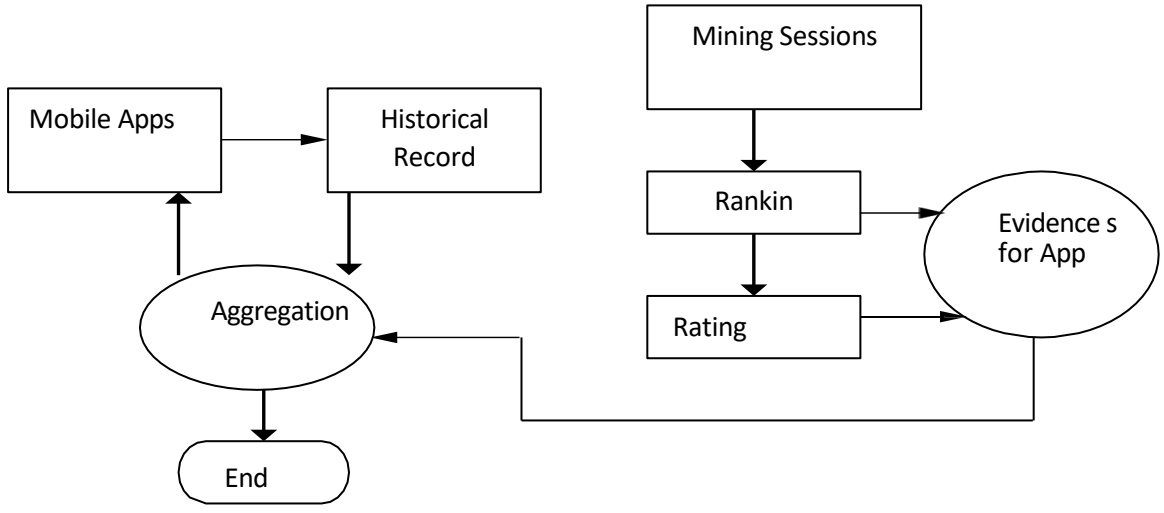
Outputs can differ in several ways, like their content, how often they're generated, when they're delivered, and in what format. The people who receive and use the system's output are the ones who validate whether the system is serving its purpose. If the output isn't up to par in any way, the system itself could be seen as failing.

To make sure the system meets its basic goals, the output must always be
Accurate: The information should always be correct.
Timely: It should be provided when it's needed.

Appropriate: The format, content, and layout should suit the purpose of the output.

APPENDICES

IV. DATA FLOW DIAGRAM



IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13362

V. CONCLUSION

This paper proposes a solution for permission tracking and the use of permissions installed in android applications. The proposed framework identifies the apps installed and its behavior according to the permission granted upon installation. This real time tracking framework monitors the installed apps for any violation in the permissions agreed. This help user identify the malicious activity and its real intention on the data usage and permissions. This app avoids the file and folder access via the malicious app by checking the permission level of that app. Also using this app we can identify the strength and weakness of android app with respect to its functionality and approach on information gathering.

REFERENCES

[1]. Jesus Castagnetto, Sascha Schumann," Proffesional Php Programming", Addison wosley Publication, Fifth Edition.
[2]. Jay Greenspan, Brad Bulgar ,"Mysql/Php Database Applications",Tata McGraw-Hill Publishing Company, Third Edition.
[3]. William Stallings,"Cryptography And Network Security",Tata McGraw-Hill Publishing Company, Third Edition.
[4]. Rogres Pressman,"Software Engineering And Applications", Galgo tie Publication, Sixth Edition
[5]. Richard Fairley,"Software Engineering Concepts",Tata McGraw-Hill Publishing Company, Fourth Edition.
[6]. Ellias M.Award "System Analysis And Design" Tata McGraw-Hill Publishing Company, Second Edition.