Analysis and identification of malicious mobile application.

Names:
Sarvadnya parad (Member)
(AM21059)
Rohit selokar (**Team leader**)
(AM21058)
Kartik karatbhajne(Member)
(AM21062)

INTRODUCTION

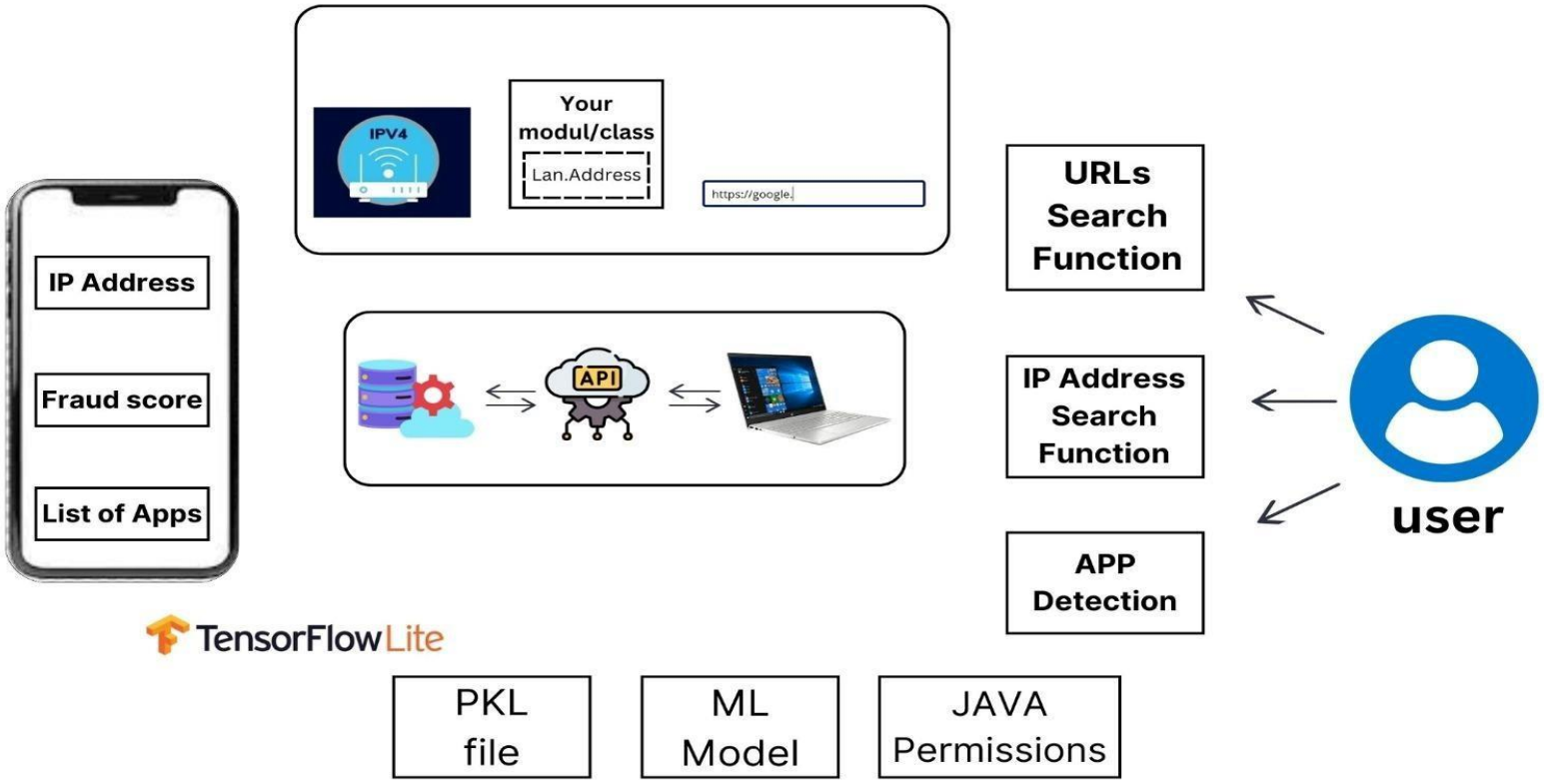
In todays era, **over 6.8 billion smartphone users worldwide** the usages of smart phone are increasing steadily, and also the growth of Android applications users are increasing.

Due to growth of android application users, some intrudes are creating malicious android application as tools to steal sensitive data and identity theft/fraud mobile bank, mobile wallets.

MOBILE DEFENDER

Working diagram

MOBILE DEFENDER



Methodology:

- 1.Data Collection:
- - Gather a diverse set of mobile applications from different sources, including app stores, third-party repositories, and research datasets.
- - Collect metadata such as app name, developer information, download count, ratings, and permissions requested.
- 2. Static Analysis:
- - Examine the app's code, including bytecode, scripts, and embedded components, to identify suspicious patterns, obfuscation techniques, and known malware signatures.
- - Analyze the permissions requested by the app to assess its access to sensitive data and system resources.
- - Check for vulnerable third-party libraries and components that may introduce security risks.

3. Behavioral Analysis:

- Identify suspicious or unexpected behavior, such as excessive battery consumption, background activities, and aggressive advertising practices.

4. Machine Learning and AI Techniques:

- Apply machine learning and artificial intelligence techniques to analyze large datasets of mobile applications and identify patterns indicative of malicious behavior.
- Train models to classify apps based on features such as permissions, code structure, and runtime behavior.
- Utilize anomaly detection algorithms to detect deviations from normal behavior and flag potentially malicious apps.
- 5. Threat Intelligence Integration:
- Incorporate threat intelligence feeds and databases into the analysis process to identify known malware signatures, indicators of compromise (IoCs), and emerging threats.
- Cross-reference analysis results with threat intelligence sources to prioritize and validate findings.

6. Reporting and Remediation:

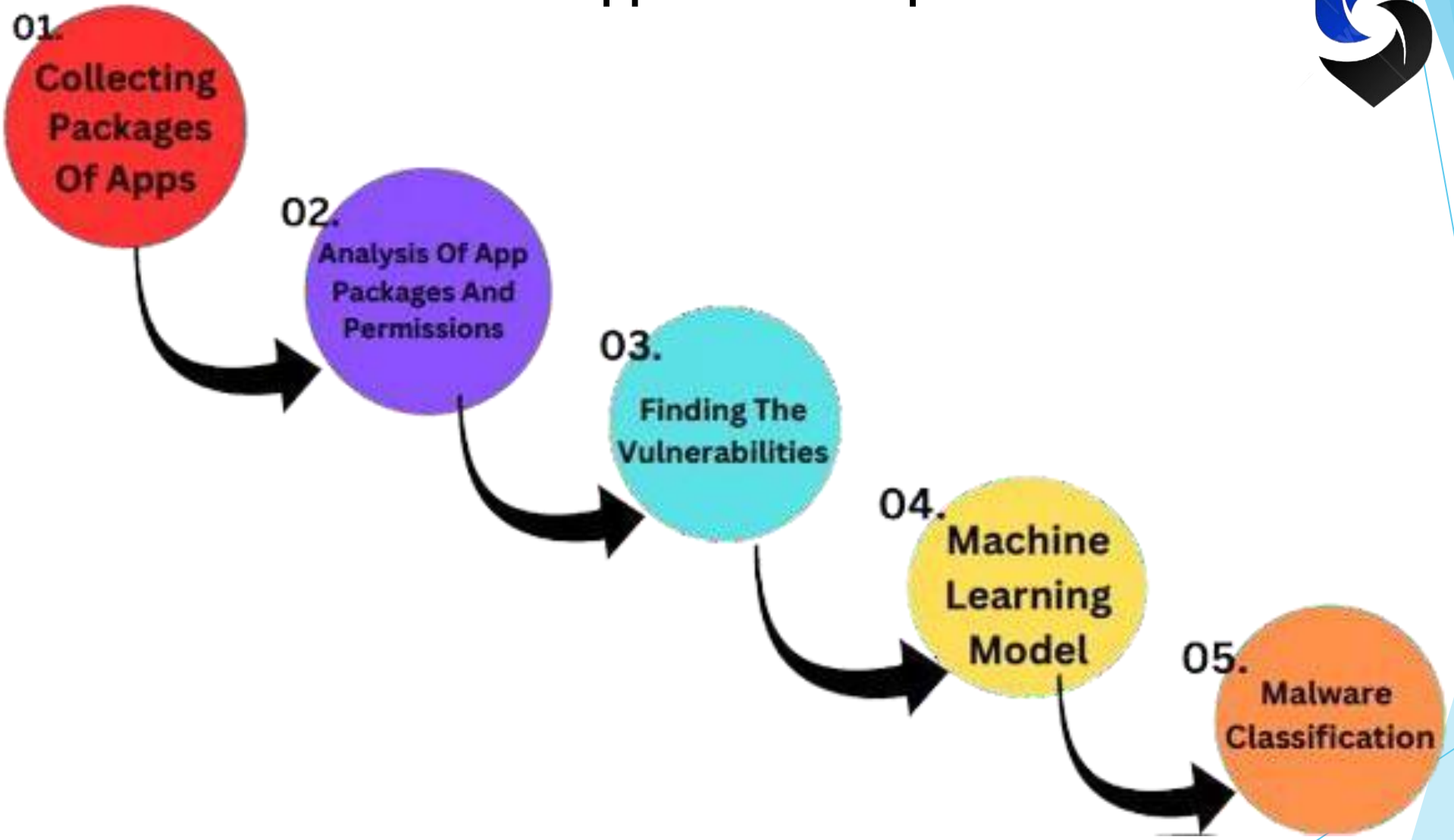
- - Document analysis findings, including identified vulnerabilities, suspicious behavior, and potential security risks.
- - Generate comprehensive reports summarizing the analysis results, actionable insights, and recommendations for remediation.

7. Continuous Monitoring and Updates:

- - Establish a process for continuous monitoring of mobile applications to detect new threats and vulnerabilities.
- - Regularly update analysis tools, techniques, and threat intelligence sources to adapt to evolving threats and maintain effectiveness over time.
- - Foster collaboration and information sharing within the security community to stay abreast of emerging trends and developments in mobile security.

Identification of application steps:

MOBILE DEFENDER



Expected Outcome :

MOBILE DEFENDER

1. Detection of Malicious Behavior:

- - Identification of mobile applications exhibiting suspicious or malicious behavior, such as data theft, unauthorized access, or intrusive advertising.
- - Detection of potentially harmful actions, including malware distribution, phishing attempts, and exploitation of vulnerabilities.

2. Classification of Threat Severity:

- - Classification of malicious applications into different threat categories, such as adware, spyware, ransomware, trojans, or potentially unwanted programs (PUPs).

3. Risk Assessment and Prioritization:

- - Evaluation of the risk posed by malicious mobile applications to users, devices, networks, and organizational assets.
- - Prioritization of remediation efforts based on the severity of identified threats, potential impact on security posture, and urgency of response.

Expected Outcome :

MOBILE DEFENDER

4. Recommendations for Remediation:

- - Provision of actionable insights, recommendations, and mitigation strategies to address identified security vulnerabilities and threats.

5. Reporting and Documentation:

- - Preparation of comprehensive reports summarizing analysis findings, including detailed descriptions of identified threats, analysis methodologies, and recommended remediation actions.
- - Documentation of analysis results, including malware samples, forensic artifacts, and evidence of malicious activity, to support incident response and forensic investigations.

6. Enhanced Security Posture:

- - Strengthening of organizational security posture through proactive identification and mitigation of mobile security threats.
- - Implementation of security controls, policies, and procedures to prevent, detect, and respond to malicious mobile applications effectively.

Thank You.