Behavioral Model for Live Detection of Apps Based Attack

[1] Balla Vani, [2] Vaddi Srivalli Devi

[1] M.C.A Student, B V Raju College, Bhimavaram, A.P, India

[2] Associate professor, Department of M.C.A, B V Raju College, Bhimavaram, A.P, India

Abstract- Smart phones with the platforms of applications are gaining extensive attention and popularity. The enormous use of different applications has paved the way to numerous security threats. The threats are in the form of attacks such as permission control attacks, phishing attacks, spyware attacks, botnets, malware attacks, privacy leakage attacks. Moreover, other vulnerabilities include invalid authorization of apps, compromise on the confidentiality of data, invalid access control. In this paper, an application-based attack modeling and attack detection is proposed. Due to A novel attack vulnerability is identified based on the app execution on the smart phone. The attack modeling involves an end-user vulnerable application to initiate an attack. The vulnerable application is installed at the background end on the smart phone with hidden visibility from the end-user. Thereby, accessing the confidential information. The detection model involves the proposed technique of an Application-based Behavioral Model Analysis (ABMA) scheme to address the attack model. The model incorporates application-based comparative parameter analysis to perform the process of intrusion detection. The ABMA is estimated by using the parameters of power, battery level, and the data usage. Based on the source internet accessibility, the analysis is performed using three different configurations as, WiFi, mobile data, and the combination of the two. The simulation results verify and demonstrate the effectiveness of the proposed model.

Index Terms—Security, attack modeling, intrusion detection, smart phone applications, Application-based Behavioral Model Analysis (ABMA), energy consumed

I. Introduction

In recent years smart phone application models have explosively increased from personnel to professional applications including education, online shopping, net banking, and healthcare. The platform of these applications has massively increased the threat of attacks by compromising trustworthiness and security capabilities. Third party application marketing is one of the major threats, wherein interested application can be installed by the end-user. However, the applications from these platforms can prove menaces with the advent of vulnerable breaches. Various attacks were identified that can prove detrimental and have adverse effects on the overall security of the information concerned to the smart phone. The jamming attack is one of the prime issues against time-critical applications.

1.1 Problem Statement

With the rapid growth of mobile and web applications, there has been a significant increase in apps-based attacks, including malware injection, phishing, privilege escalation, and unauthorized access to sensitive user data. Traditional security mechanisms often rely on static or signature-based detection methods, which are ineffective against novel, zero-day, or behaviorally subtle threats. These approaches also struggle to provide real-time protection due to their dependence on predefined attack signatures or manual intervention.

There is a critical need for **a** behavioral model that can detect apps-based attacks in real time by analyzing the dynamic behavior of applications during runtime. Such a model should be capable of distinguishing between normal and malicious behavior patterns by leveraging techniques like anomaly detection, machine learning, and context-aware analysis. The primary challenge lies in accurately identifying malicious behaviors without causing high false positive rates, while ensuring minimal performance overhead and preserving user privacy.

1.2 Purpose:

The purpose of this study is to develop a behavioral-based detection model that can identify and prevent apps-based attacks in real time by analyzing the runtime behavior of applications. Unlike traditional signature-based methods, this model will focus on detecting anomalous patterns and activities that deviate from normal application behavior, enabling it to recognize new, unknown, or evolving threats. This behavioral model aims to:

- Enhance real-time detection capabilities against attacks such as privilege abuse, unauthorized access, and data exfiltration.
- Reduce false positives by understanding the context and intent of app actions.
- Offer a lightweight and scalable solution suitable for deployment on mobile devices, servers, or cloud environments.

1.3 Scope:

This study focuses on the design, development, and evaluation of a behavioral model for the live detection of attacks originating from or executed through applications, particularly in dynamic environments like mobile platforms, web applications, or cloud-based systems.

1.4 Motivation:

The motivation behind this study is to bridge the gap between reactive security measures and proactive behavioral-based protection, providing users and systems with a more robust, accurate, and timely defense mechanism against modern and emerging apps-based cyber threats.

1.5 Overview:

The Behavioral Model for Live Detection of Apps-Based Attacks is a proactive security framework designed to monitor and analyze the runtime behavior of applications in real-time, with the objective of identifying malicious or abnormal activities that may indicate an ongoing attack. Unlike traditional detection systems that rely on static signatures or predefined rules, this model focuses on dynamic analysis, capturing how an application interacts with the system, network, and user data during execution.

II. Related Work

The growing reliance on mobile and web applications has significantly increased the attack surface for cyber threats. Researchers and security experts have explored various techniques to detect and mitigate such threats, broadly categorized into signature-based**,** static analysis**,** dynamic (behavioral) analysis**, and** hybrid approaches**.**

1. Signature-Based and Static Analysis Approaches

Signature-based detection, such as that used by traditional antivirus systems, relies on known attack patterns or malware signatures. Tools like **ClamAV** and **VirusTotal** operate in this category. While effective against known threats, these systems fail against **zero-day attacks** or **polymorphic malware**, as highlighted by [Santos et al., 2013].

Static analysis involves examining the source code or application binary without executing it. Frameworks like **Androguard** and **FlowDroid** have been developed to analyze Android apps for vulnerabilities. However, static techniques often struggle with **code obfuscation**, **dynamic loading**, and **runtime behavior**, limiting their ability to detect advanced threats.

2. Dynamic and Behavioral Detection Models

Behavioral analysis involves monitoring app behavior during execution to detect anomalies. **Tam et al. (2015)** introduced a dynamic malware detection model based on system call monitoring and anomaly detection. Similarly, **Enck et al. (2010)** developed **TaintDroid**, a real-time privacy monitoring system for Android that tracks sensitive data flows.

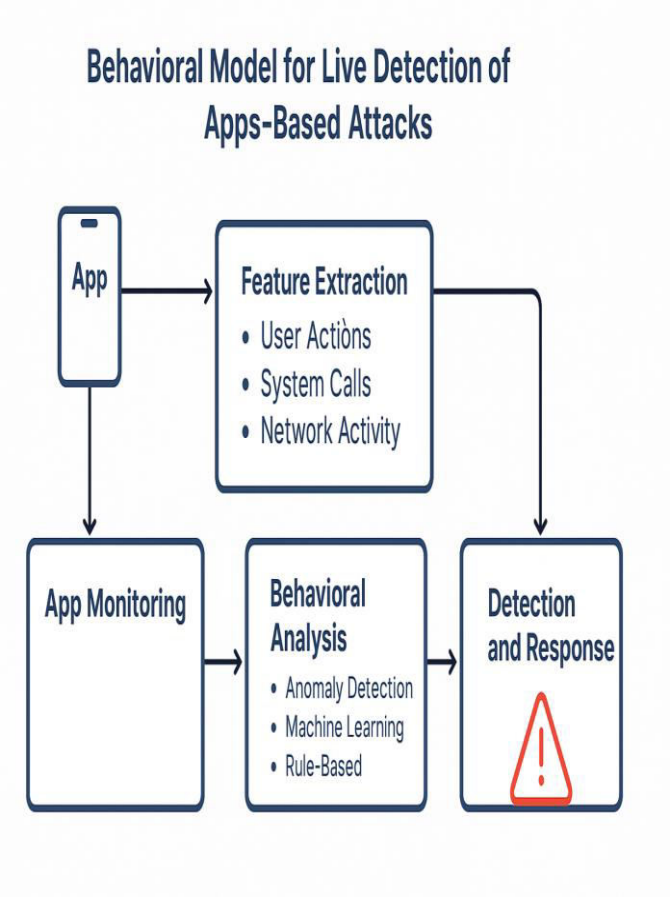
Machine learning-based approaches have shown promise in this space. **Arp et al. (2014)** proposed **Drebin**, a lightweight Android malware detector using static features and machine learning. Although Drebin was efficient, it lacked the ability to monitor real-time behavior.

III. PROPOSED SYSTEM

Application-based Behavioral Model Analysis (ABMA) is a novel methodology defined for security improvement of smartphone platforms. Conventional schemes of security enhancement mechanisms in smartphones are attack-specific or application-specific. A generalized security scheme independent of versions and type of application is yet to be addressed. Also, the reliability with upgradation and optimized statistical parameters require immense attention. The behavioral model for smartphone based applications is an innovative initiative to address these challenges with an effectual performance. The model is independent of the technology and the updates of the applications of the smartphone. It provides the live detection app based attack with adaptive capability. The detection model ensures the apps based attack detection on authorization, confidentiality, and integrity with efficient and less complex methodology.

Advantages:

- A novel and probable application-based attacking model has been identified with an efficient strategy of hidden access installation in the background and the hidden visibility from the end-user.
- The detection model for the applications of the smart phone has been proposed to address the modeled attack. The evaluation is based on the comparative analysis of the behavioral model such that the actual parameters are compared with the parameters in presence of the intruder application.
- To counteract the detected intrusion, an alarm is raised as the immediate response followed by the disconnection of the cellular services and internet accessibility.
- The obtained results illustrate that the proposed scheme can prove an effective mechanism using ABMA in terms of power, data, and battery level.



IV. CONCLUSION

In an era where applications serve as a primary interface between users and digital ecosystems, securing these apps against sophisticated attacks has become more critical than ever. The proposed behavioral model for live detection of apps-based attacks offers a proactive and adaptive approach to identifying malicious behavior by continuously monitoring and analyzing application activity in real-time.Unlike traditional static or signature-based detection methods, this model emphasizes dynamic behavior profiling and anomaly detection to uncover threats that may bypass conventional defenses, including zero-day exploits and misuse of legitimate app functionalities. By leveraging machine learning and temporal analysis, the model builds intelligent, evolving baselines that can distinguish between benign anomalies and truly malicious activities.This approach not only enhances the speed and accuracy of threat detection but also reduces the dependency on predefined signatures, enabling systems to remain resilient in the face of ever-evolving cyber threats. With careful consideration of privacy, resource efficiency, and continuous feedback integration, this behavioral model holds significant promise for strengthening app security across mobile and enterprise environments.

Future work will focus on optimizing detection algorithms for low-latency environments, enhancing model explainability, and integrating federated learning to preserve user privacy while benefiting from collective intelligence.

V. REFERENCES

[1] M. S. Abdalzaher and O. Muta, "A Game-Theoretic Approach for Enhancing Security and Data Trustworthiness in IoT Applications," in *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11250-11261, Nov. 2020.

[2] C. Shen, Y. Chen, Y. Liu and X. Guan, "Adaptive Human–Machine Interactive Behavior Analysis With Wrist-Worn Devices for Password Inference," in *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 12, pp. 6292-6302, Dec. 2018.

[3] W. Wang, X. Wang, D. Feng, J. Liu, Z. Han and X. Zhang, "Exploring Permission-Induced Risk in Android Applications for Malicious Application Detection," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1869-1882, Nov. 2014.

[4] Z. Lu, W. Wang and C. Wang, "Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications," in *IEEE*

Transactions on Mobile Computing, vol. 13, no. 8, pp. 1746-1759, Aug. 2014.

[5] J. Mao, S. Zhu, X. Dai, Q. Lin and J. Liu, "Watchdog: Detecting Ultrasonic-Based Inaudible Voice Attacks to Smart Home Systems," in *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8025-8035, Sept. 2020.

[6] L. Wu, X. Du and X. Fu, "Security threats to mobile multimedia applications: Camera-based attacks on mobile phones," in *IEEE Communications Magazine*, vol. 52, no. 3, pp. 80-87, March 2014.

[7] R. Spreitzer, V. Moonsamy, T. Korak and S. Mangard, "Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices," in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 465-488, Firstquarter 2018.

[8] A. Maiti, M. Jadliwala, J. He and I. Bilogrevic, "Side-Channel Inference Attacks on Mobile Keypads Using Smartwatches," in *IEEE Transactions on Mobile Computing*, vol. 17, no. 9, pp. 2180-2194, 1 Sept. 2018.

[9] S. Naval, A. Pandey, S. Gupta, G. Singal, V. Vinoba and N. Kumar, "PIN Inference Attack: A Threat to Mobile Security and Smartphone-controlled Robots,"in *IEEE Sensors Journal*, 2021. doi: 10.1109/JSEN.2021.3080587.

[10] J. Yu, L. Lu, Y. Chen, Y. Zhu and L. Kong, "An Indirect Eavesdropping Attack of Keystrokes on Touch Screen through Acoustic Sensing," in *IEEE Transactions on Mobile Computing*, vol. 20, no. 2, pp. 337-351, 1 Feb. 2021.

[11] Y. Zhang, M. Yang, G. Gu and H. Chen, "Rethinking Permission Enforcement Mechanism on Mobile Systems," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 10, pp. 2227-2240, Oct. 2016.

[12] F. Roesner, "Designing Application Permission Models that Meet User Expectations," in *IEEE Security & Privacy*, vol. 15, no. 1, pp. 75-79, Jan.-Feb. 2017.