IDS For Mobile Devices

Kunduru Nikunj Raghav (CB.EN.U4CSE19030)
Penugonda Sai Koushik (CB.EN.U4CSE19449)
Ravella Abhinav (CB.EN.U4CSE19453)
Singadi Shanthan Reddy (CB.EN.U4CSE19459)

Project Mentor: Dr. Senthil Kumar T., Associate Professor,
Dept. of Computer Science & Engineering
Amrita School of Computing
Amrita Vishwa Vidyapeetham

08 December 2022

Abstract

This paper presents an intrusion detection system designed to detect malicious activities on mobile devices. The system is designed to detect and identify anomalies in the mobile device's network traffic, application usage, and system events. It uses a variety of techniques to detect suspicious activities, such as deep packet inspection, traffic analysis, and pattern matching. The system also uses a variety of methods to analyze and classify the data, including machine learning algorithms, statistical methods, and heuristics. The system is designed to minimize false positives and false negatives, and to provide an alert when a malicious activity is detected. The system also provides detailed reports of the analysis and detected anomalies. The system is designed to be deployed on a variety of mobile platforms and can be integrated with existing security systems. The system is also designed to be scalable and able to adapt to changing mobile threats.

Keywords

Intrusion Detection, Edge Devices, Decision Tree

1 Acknowledgment

We would want to express our sincere gratitude to Dr. Senthil Kumar T., our mentor, for his important counsel and help in finishing Phase I. He challenged us to think creatively and exhorted us to act without hesitation. We would want to express our gratitude to our university for giving us the chance to work on the project (Intrusion Detection System for Mobile Devices). Finally, we would like to thank everyone who helped our project's Phase I be completed successfully as well as our parents, friends, and others for their comments.

2 Introduction

An intrusion detection system (IDS) is a technology used to monitor a network or system for malicious activities or policy violations. It is a type of security management system that identifies malicious or unauthorized activities and attempts to prevent them from occurring. An IDS can be either a software- or hardware-based system that is designed to detect malicious activity on the network by analyzing network traffic for potential threats and alerting administrators when one is detected. It is typically used to detect and respond to cyber attacks and other malicious activities, as well as to monitor user activity and detect policy violations.

2.1 Motivation

Intrusion detection systems are an important security measure for computer systems and networks. They provide a way to detect and respond to malicious activity, such as unauthorized access or data theft. They can also help

prevent future attacks by monitoring network traffic, alerting administrators to suspicious activity, and providing detailed information about potential threats. Intrusion detection systems can help organizations protect their data, reduce operational costs, and protect their users from malicious activity.

2.2 Major Contribution

- To detect various types of attacks between systems
- To analyze various logs from the devices

3 Literature Survey

S.NO	Authors Name(s)	Full title of the paper with year	Inference from the paper	Open Problem
1	Shiyi Jin, Jin-Gyun Chung, Yinan Xu	Signature-Based Intrusion Detection System (IDS) for In-Vehicle CAN Bus Network May 2021	Most of the intrusion detection solutions requiring extensive computational resources cannot be implemented in in- vehicle network system because of the resource constrain. This paper proposes a signature-based IDS to detect the anomalies on the basis for selecting signatures.	The detection is not real-time and new attacks are not detected, future works need to deal with some deep learning methods or hybrid approaches.
2	K. Hatonen, P. Halonen, M.Miettinen	Host-Based Intrusion Detection for Advanced Mobile Devices April 2006	Shows that host-based approaches are required, since network-based monitoring alone is not sufficient to encounter the future threats. We outline some of the data types on mobile devices that could be used to construct intrusion detection models, and finally propose a framework for mobile device intrusion detection.	Showed that network-based intrusion detection alone is not sufficient in the future environment and suggest therefore that they should be augmented with intrusion detection models that are host-based
3	Jitti Annie Abraham, V. R. Bindu	Intrusion Detection and Prevention i n Networks Using Machine Learning and Deep Learning Approaches October 2021	The accuracy of an intrusion detection system determines its performance. To reduce false alarms and increase detection rates, intrusion detection accuracy must be improved. The main objective is to performance comparison of different machine learning classification methods	Some machine learning algorithms have low accuracy levels, future works need to deal with some deep learning methods or hybrid approaches.
4	Bane Raman Raghunath, Shivsharan Nitin Mahadeo	Network Intrusion Detection System July 2008	Shows us anomaly detection that summarizes those network connections that are ranked highly anomalous by the anomaly detection module. Experimental results show that anomaly detection techniques are successful in automatically detecting several intrusions that could not be identified using popular signature-based tools	Analysis is not done on the device but sent over to master device which leads to big data issue

4 Proposed System

- Logs collection
- Raw data to CSV transformation
- Generate regular expression
- Test case generation
- Validation

5 Results and Analysis

- Data Successfully collected from devices
- Using parser toll transformed raw data to comma-separated values
- Used various algorithms to predict whether it is an attack or not
- Got accuracy of 91%

6 Conclusion and Future Work

The implementation of Intrusion Detection System using ML algorithms has proven successful in identifying potential threats and malicious behavior in networks. It has also been shown to reduce false positives, increase accuracy, and improve detection time. With the use of Deep Learning algorithms, the IDS can be further enhanced to provide better security and protection to networks. In conclusion, the use of Machine Learning algorithms in IDS systems is an effective way to detect and prevent malicious activities in networks.

References

1. Jieming Zhu, Shilin He, Jinyang Liu, Pinjia He, Qi Xie, Zibin Zheng, et al., "Tools and benchmarks for automated log parsing", *2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*, pp. 121-130, 2019.

2. N. Gao, L. Gao, Q. Gao and H. Wang, "An Intrusion Detection Model Based on Deep Belief Networks", *2014 Second International Conference on Advanced Cloud and Big Data*, pp. 247-252, 2014.

3. S He, J Zhu, P He et al., "Experience report: system log analysis for anomaly detection", *2016 IEEE 27th International Symposium on Software Reliability Engineering (ISSRE)*, pp. 207-218, 2016.

4. Q Fu, J G Lou, Y Wang et al., "Execution anomaly detection in distributed systems through unstructured log analysis", *2009 ninth IEEE international conference on data mining*, pp. 149-158, 2009.