Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA DOI: 10.46254/NA10.20250108
Published: June 17, 2025

Towards Intelligent Detection of Android Remote Access Trojans (RATs)

Nesreen Dalhy
MS Graduate Student
Department of Computer Science
Florida Polytechnic University
Lakeland, Florida, USA
ndalhy8095@floridapoly.edu

Karim Elish
Associate Professor
Department of Computer Science
Florida Polytechnic University
Lakeland, Florida, USA
kelish@floridapoly.edu

Abstract

Remote Access Trojans (RATs) pose a significant and persistent threat to Android security, enabling cybercriminals to gain unauthorized access to sensitive user data and control infected devices. Despite advancements in cybersecurity, detecting Android RATs remains an open challenge due to their evolving evasion techniques and stealthy behavior. Traditional detection methods often fail to keep pace with the rapid evolution of these threats; hence, there is a need for more robust and intelligent detection mechanisms. In this thesis, we propose an advanced detection framework leveraging ensemble machine learning models to effectively identify and classify Android RATs. By analyzing a diverse dataset of malicious Android applications, this study examines dynamic features such as system calls and static features like permissions, intent filters and metadata to develop a comprehensive detection approach for Android RATs. The experimental results demonstrate that XGBoost model achieves the best trade-off between precision, recall, and false positive rate, making it the most reliable model for RAT detection. Furthermore, this research incorporates optimized feature selection techniques to enhance model performance and improve detection accuracy. Additionally, we investigate the effectiveness of different Large Language Models (LLMs) in identifying Android RATs. This work provides valuable insights into the strengths and limitations of current machine learning-based approaches in detecting Android RATs by benchmarking multiple models and analyzing their comparative effectiveness. The proposed detection framework aims to enhance mobile security by equipping Android users and cybersecurity professionals with a more accurate, efficient, and adaptive solution against evolving RAT threats.

Keywords

Remote Access Trojan (RATs), Android Security, Malware Detection, Ensemble Learning, AI in Cybersecurity.

Biographies

Nesreen Dalhy is a graduate student in the Master of Computer Science program at Florida Polytechnic University. Her research focuses on detecting Android Remote Access Trojans on mobile devices. Nesreen holds a bachelor's degree in computer science with a concentration in Cybersecurity from Florida Polytechnic University and holds a CompTIA Security+ certification.

Dr. Karim Elish is an associate professor of Computer Science at Florida Polytechnic University. He obtained his Ph.D. and MS in Computer Science from Virginia Tech. Before joining Florida Poly in 2016, he was an assistant professor at the Department of Computer Science at Purdue University-Fort Wayne. He received the prestigious Florida Poly ABLAZE Award for Excellence in Teaching in 2018. Dr. Elish's research portfolio is centered at the intersection of cybersecurity and software engineering. His expertise encompasses a wide array of topics, including cybersecurity analytics, software security, mobile security, and applied AI and ML. His work in these areas has garnered substantial recognition, with over 1,630+ citations on Google Scholar. He also has showcased his proficiency in acquiring funding, securing a total of around $716,000 in grants as both PI and Co-PI. Dr. Elish is serving as a reviewer for many high impact ISI journals and conferences such as IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE Transactions on Information Forensics & Security, IEEE Transactions on Mobile computing (TMC), and others. He holds senior membership in both IEEE and ACM.