INFUSE 2025: International Conference on Frontiers of Unified Science and Exploration

Contribution ID: **138** Type: **Poster**

Malware Reverse Engineering: Static Analysis for Threat Detection

Malware reverse engineering through static analysis is a vital cybersecurity process that involves dissecting malicious software, such as viruses, ransomware, and trojans, without executing them to uncover their design, functionality, and attack vectors. By employing tools like disassemblers and decompilers, analysts examine binaries or Android APKs, scrutinizing elements like the AndroidManifest.xml for suspicious permissions or code for obfuscated logic, enabling rapid identification of threats through comparison with malware signatures. This safe and efficient method supports initial triage and large-scale analysis but struggles with runtime behaviors and advanced obfuscation, necessitating complementary dynamic and manual analysis for comprehensive threat mitigation. As Android remains a prime target, static analysis, enhanced by evolving tools and threat intelligence, strengthens detection and countermeasures, safeguarding digital systems from sophisticated cyberattacks.

Keywords: Malware, Reverse Engineering, Static Analysis, Cybersecurity, Android APKs, Decompilers, Disassemblers, AndroidManifest.xml, Obfuscation, Threat Intelligence, Malware Signatures, Dynamic Analysis, Cyberattacks, Detection, Countermeasures.

Author: MUKHERJEE, MONAMI (JAIN (Deemed-to-be University))

Co-author: Mr NATARAJAN, VISHNU VENKATESH (JAIN (Deemed-to-be University))

Presenter: MUKHERJEE, MONAMI (JAIN (Deemed-to-be University))

Track Classification: Forensic Sciences