Engineering Village™

1. **Deep Learning for Android Malware Defenses: a Systematic Literature Review [arXiv]**
Yue Liu; Tantithamthavorn, C.; Li Li; Yepang Liu **Source:** *arXiv*, 51 pp., 9 March 2021; **Publisher:** arXiv, USA

Author affiliation:
Monash University, Melbourne, VIC, Australia
Southern University of Science and Technology, China

Abstract: Malicious applications (especially in the Android platform) are a serious threat to developers and end-users. Many research efforts have hence been devoted to developing effective approaches to defend Android malware. However, with the explosive growth of Android malware and the continuous advancement of malicious evasion technologies like obfuscation and reflection, android malware defenses based on manual rules or traditional machine learning may not be effective due to limited apriori knowledge. In recent years, a dominant research field of deep learning (DL) with the powerful feature abstraction ability has demonstrated a compelling and promising performance in various fields, like Nature Language processing and image processing. To this end, employing deep learning techniques to thwart the attack of Android malware has recently gained considerable research attention. Yet, there exists no systematic literature review that focuses on deep learning approaches for Android Malware defenses. In this paper, we conducted a systematic literature review to search and analyze how deep learning approaches have been applied in the context of malware defenses in the Android environment. As a result, a total of 104 studies were identified over the period 2014-2020. The results of our investigation show that even though most of these studies still mainly consider DL-based on Android malware detection, 35 primary studies (33.7\%) design the defenses approaches based on other scenarios. This review also describes research trends, research focuses, challenges, and future research directions in DL-based Android malware defenses. (0 refs.) **Inspec controlled terms:** invasive software - learning (artificial intelligence) - natural language processing

Uncontrolled terms: systematic literature review - deep learning approaches - Android environment - Android malware detection - Android platform - dominant research field - deep learning techniques

Classification Code: C6130S Data security - C6180N Natural language processing

IPC Code: G06F17/20 - G06F21/00 - G06N20/00

Treatment: Bibliography (BIB); Practical (PRA)

Database: Inspec