롱 숏 텀 메모리를 활용한 권한 기반 안드로이드 말웨어 자동 복구

오지강[O], 천 신[*], 이욱진[*]
[O*]한양대학교 컴퓨터공학과
e-mail: {wzq0515[O], xxtx0122[*], scottlee[*]}@hanyang.ac.kr

Permissions based Automatic Android Malware Repair using Long Short Term Memory

Zhiqiang Wu[O], Xin Chen[*], Scott Uk-Jin Lee[*]
[O*]Dept. of Computer Science and Engineering, Hanyang University

● 요 약 ●

As malicious apps vary significantly across Android malware, it is challenging to prevent that the end-users download apps from unsecured app markets. In this paper, we propose an approach to classify the malicious methods based on permissions using Long Short Term Memory (LSTM) that is used to embed the semantics among Intent and permissions. Then the malicious method that is an unsecured method will be removed and re-uploaded to official market. This approach may induce that the end-users download apps from official market in order to reduce the risk of attacks.

키워드: Malware Detection, Software Repair, Android Security

I. Introduction

Android is the most popular smart mobile device platform in the world. There are millions apps available in Google Play and other third-parties. Unlike other mobile systems, Android Operating System allows end users to download the unverified apps from third-parties. The end-users usually do not have enough professional knowledge to avoid these threats if they do not know Android security, which leads to the mobile devices at the risk. There is not an alternative app in official market, so that the end-users may download required apps from an unsecured party.

To address this security concern, we propose an approach to automatically repair Android malware based on permissions. The LSTM applied to build the relationship by semantics between permission definition in manifest.xml file and called intents in method level source code. The permissions that utilized by malicious method can be removed and uploaded to official market.

II. Related Workds

There are various malware detection techniques for Android apps using static and dynamic analysis. The existing approaches can achieve higher accuracy by various features of Android. DeepRefiner [1] applied deep neural networks to classify Android malware based on both xml files and bytecode of methods with the accuracy of 97%, which is able to embed the semantics of bytecode to classify the apps. Although there are existing various approaches with the high accuracy such as SALMA [2], the mobile devices still suffer from the risk of malware because we cannot prevent the end-users to download these malicious apps.

III. The Proposed Scheme

The architecture of overall repair system is shown in Fig. 1.

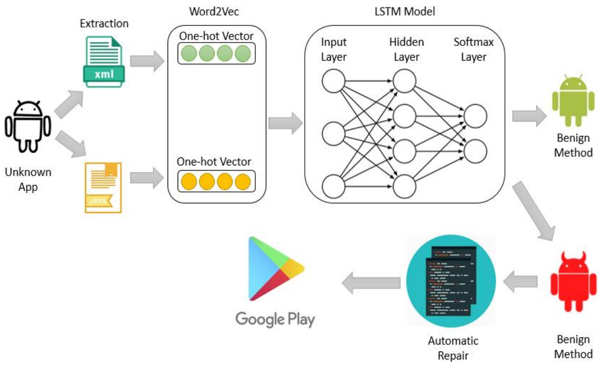

Fig. 1. System Architecture

1.1 Preprocessing

We collect the Android malware that are verified by VirusShare [3]. We only extract the two kinds of features from permissions and Intent by decompiling the Android apk in order to classify malicious or benign methods.

Permissions: Permissions are defined in xml file which includes the whole information about the application. The permissions can be easily extract by XML tag.

Intent: The intents only exist in the method level code. Therefore, our approach will analyze all java files to extract called system services.

1.2 Word2Vec and Identification

Word2Vector applied for transforming the code into one-hot vector. To this end, the system builds two dataset according to the unique permission values and Intents retrieved from training dataset. Then, the LSTM adopted to embed the semantics of Intents and build the relevance among permission vector and Intent vectors. As a result, the malicious method can be classified by Softmax.

1.3 Automatic Repair

If the permission used for a malicious method in app, this malicious method will be removed in this part. The malicious method may be directly removed, then this app will be repacked and uploaded to official market.

IV. Conclusions

In this paper, we proposed a permission based approach to find out the malicious method and automatically repair the malicious code using LSTM technique. As the growth rate of Android malware, millions apps produced in Google Play. However, it could not satisfy that the various requires of end-users. Our approach can remove those malicious methods and upload to official market, which may induce that the end-users download apps from official market.

Acknowledgement

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korean government (MSIP) (No. NRF-2016R1C1B2008624).

REFERENCES

[1] K. Xu, Y. Li, R. H. Deng and K. Chen, "DeepRefiner: Multi-layer Android Malware Detection System Applying Deep Neural Networks", in Proc. of the IEEE European Symposium on Security and Privacy, pp. 473-487, 2018

[2] M. Hammad, J. Garcia and S. Malek, "Self Protection of Android Systems from Inter-component Communication Attacks", in Proc. of International Conference on Automated Software Engineering, pp. 726-736, 2018

[3] VirusShare, https://virusshare.com/