DroidDetector: Android Malware Characterization and Detection Using Deep Learning

Fangfang Li

June 2, 2018

1. Feature Extraction

To systematically characterize Android apps, we conduct static and dynamic analyses to extract features from each app, as shown in Fig. 1. All the features fall under one of three types: required permissions, sensitive APIs, and dynamic behaviors [1]. Among them, required permissions and sensitive APIs are extracted through the static analysis, whereas dynamic behaviors are extracted through dynamic analysis. Specifically, all we need is the installation file of each Android app.

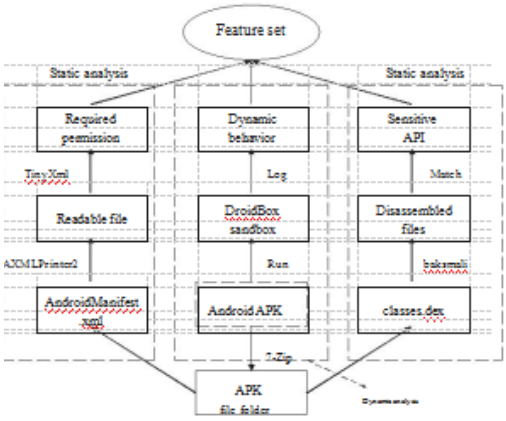

Figure 1. Feature extraction for an Android app.

2. Deep Learning Engine

Traditional machine learning models that have less than three layers of computation units are considered to have shallow architectures. Fortunately, deep learning models with a deep architecture change that situation. In practical use, a deep learning model can be constructed with different deep architectures. Deep Belief Networks (DBN) and convolutional neural networks. For this study, we chose DBN architecture to construct our deep learning model and characterize Android apps.

As shown in Fig. 2, the construction of a deep learning model has two phases, the unsupervised pre-training phase and supervised back-propagation phases [3]. In the pre-training phase, the DBN is hierarchically built by stacking a number of Restricted Boltzmann Machines (RBM), with the deep neural network regarded as a latent variable model, which is beneficial for gradually evolving high-level representations. In the back-propagation phase, the pre-trained DBN is fine-tuned with labeled samples in a supervised manner. The deep learning model uses the same app set in both phases of the training process. In this way, the deep learning model is completely built.

We implemented the Android malware detection engine DroidDetector based on the deep learning [2].

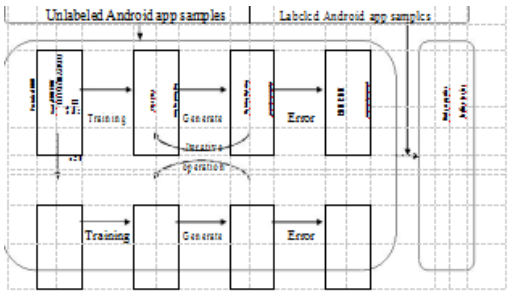

Figure 2. Deep learning model constructed with DBN.

References

[1] I. Goodfellow, Y. Bengio, A. Courville, and Y. Bengio. *Deep learning*, volume 1. MIT press Cambridge, 2016. 1

[2] A. Krizhevsky, I. Sutskever, and G. E. Hinton. Imagenet classification with deep convolutional neural networks. In *IEEE Conference on Computer Vision and Pattern Recognition(CVPR)*, pages 1097–1105, 2012. 1

[3] J. Schmidhuber. Deep learning in neural networks: An overview. *Neural networks*, 61:85–117, 2015. 1