MACHINE LEARNING IN ANDROID MALWARE EVASION

Trần Tấn Hải
21522036

Bùi Nguyên Phúc
21522469

Huỳnh Anh Nguyễn
21522388

Khoa Mạng máy tính và Truyền thông, Trường Đại học Công nghệ Thông tin – ĐHQG-HCM

GIỚI THIỆU

Hiện nay các thiết bị mobile đang càng ngày phổ biến (smartphone, tablet, ...) và phần lớn các thiết bị này chạy hệ điều hành Android. Nên việc mã độc càng phổ biến trên nền tảng này là điều hiển nhiên. Tuy nhiên các giải pháp Machine Learning được áp dụng vào việc tự động phát hiện mã độc trên nền tảng này cũng đang được phát triển liên tục và đã có được một vài kết quả tốt. Như hai Android Malware Detection Schemes: MaMaDroid và Drebin có tỉ lệ phát hiện mã độc là 96%, 97%.
Mục tiêu của đồ án sẽ là tạo một chương trình có khả năng tạo mẫu mã độc đột biến có khả năng trốn tránh các trình phát hiện mã độc trên nền tảng Android (cụ thể ở đây là MaMaDroid)

CƠ SỞ LÝ THUYẾT

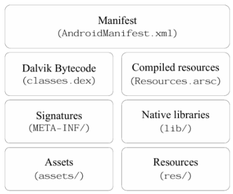


Figure 1: Cấu trúc file APK

MaMaDroid và Drebin là công cụ trích xuất đặc trưng sử dụng machine learning giải quyết bài toán phần lớp nhị phân (binary classification) phân biệt file mã độc và file bình thường.

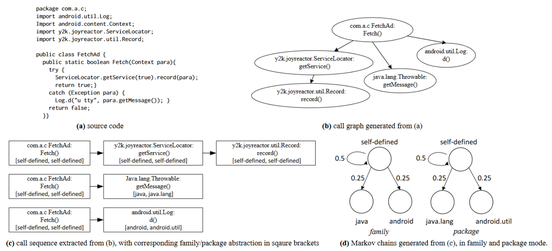


Figure 2: Quá trình MaMaDroid trích xuất đặc trưng

Figure 3: Cách MaMaDroid trích xuất API call

Ta sẽ tấn công bằng việc tính toán số lượng API call và làm nhiễu chuỗi API call với thuật toán C&W từ đó làm nhiễu vector đặc trưng để MaMaDroid không nhận diện đây là file mã độc.

PHƯƠNG PHÁP THỰC HIỆN

DATASET

https://www.kaggle.com/datasets/shashwatwork/android-malware-dataset-for-machine-learning

Ta sẽ tải vài file APK malware về để cho quá trình thực nghiệm chỉnh sửa file malware sao cho có thể tránh né trình phát hiện.

Tên Dataset	drebin215dataset5560malware9476benign
Số lượng đặc trưng	215
Số lượng dòng	15036
Lớp	Benign, Malicious
Số lượng file Benign	9476
Số lượng file Malicious	5560

MAMADROID

https://bitbucket.org/gianluca_students/mamadroid_code/src/master

Drebin

https://github.com/annamalai-nr/drebin

C&W ATTACK MODEL

https://github.com/zacharykzhao/AndroidHIV/tree/main

JSMA ATTACK MODEL

https://github.com/hai2036/NT522.O21.ATCL-Machine-Learning-in-Android-Malware-Evasion

Classifier algorithm	Support Vector Machine (SVM)
Kernel	Linear
C	1

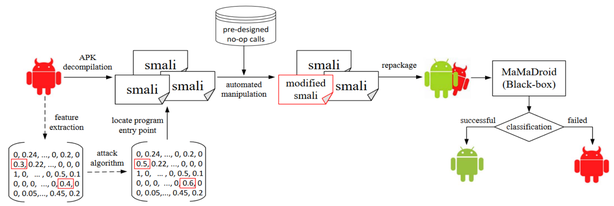


Figure 4: Quá trình thử nghiệm

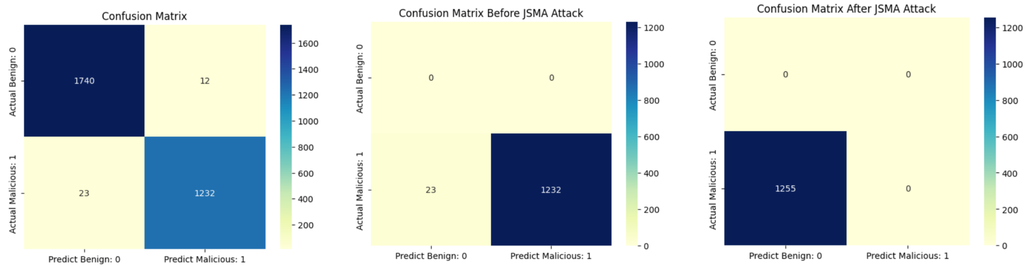
MÔI TRƯỜNG

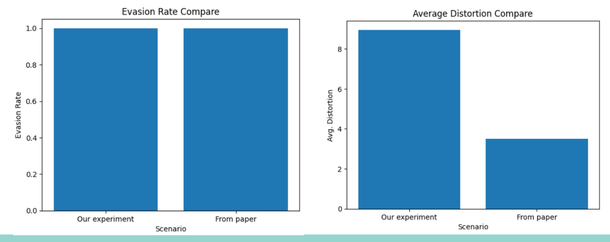
Jupyter Notebook - Visual Studio Code
CPU: 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz
RAM: 8GB
OS: Windows 10 Home Single Language

Attack algorithm	JSMA
Classifier	SVM
theta	0.1
gamma	1
batch_size	1

KẾT QUẢ

https://github.com/hai2036/NT522.O21.ATCL-Machine-Learning-in-Android-Malware-Evasion





KẾT LUẬN & HƯỚNG PHÁT TRIỂN

KẾT LUẬN

Qua đồ án này ta có thể thấy được các trình phát hiện mã độc dựa trên các mô hình machine learning đơn giản vẫn có điểm yếu trước các mẫu mã độc đối kháng nói chung, trên nền tảng Android nói riêng. Điểm yếu này là một điểm yếu chí mạng đối với các hệ thống phụ thuộc vào nó, nên ta cần có các giải pháp hợp lý như sử dụng các mẫu mã độc đối kháng để huấn luyện cho mô hình machine learning. Đồ án này đã thể hiện rất rõ sự hiểu quả của mẫu đối kháng có hiệu quả như thế nào trong việc đánh lừa hệ thống phát hiện mã độc trên nền tảng Android.

HƯỚNG PHÁT TRIỂN

Có thể xây dựng thành một ứng dụng web giống như trang virustotal.com ta chỉ cần chọn detection file APK malicious hay benign thì bỏ vào web sẽ cho ta kết quả. Nếu chọn evasion thì chỉ cần bỏ file APK malicious vào thì web sẽ tự động trả về 1 file APK malicious đã được chỉnh sửa để có thể né được phần detection của web.

REFERENCES

X. Chen et al., "Android HIV: A Study of Repackaging Mal-ware for Evading Machine-Learning Detection," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 987-1001, 2020, doi: 10.1109/TIFS.2019.2932228.