PHÂN TÍCH MÃ ĐỘC ANDROID BẰNG MÔ HÌNH GENERATIVE ADVERSARIAL NETWORKS

NGUYỄN VĂN VƯỢNG - 250201040

GVHD: PGS. TS. Lê Đình Duy

Tóm tắt

- Lớp: CS2205.CH201
- Link Github của nhóm: https://github.com/Vuoncog/ResearchMethod
- Link YouTube video: https://youtu.be/Gw6rLfohxqA
- Nguyễn Văn Vượng

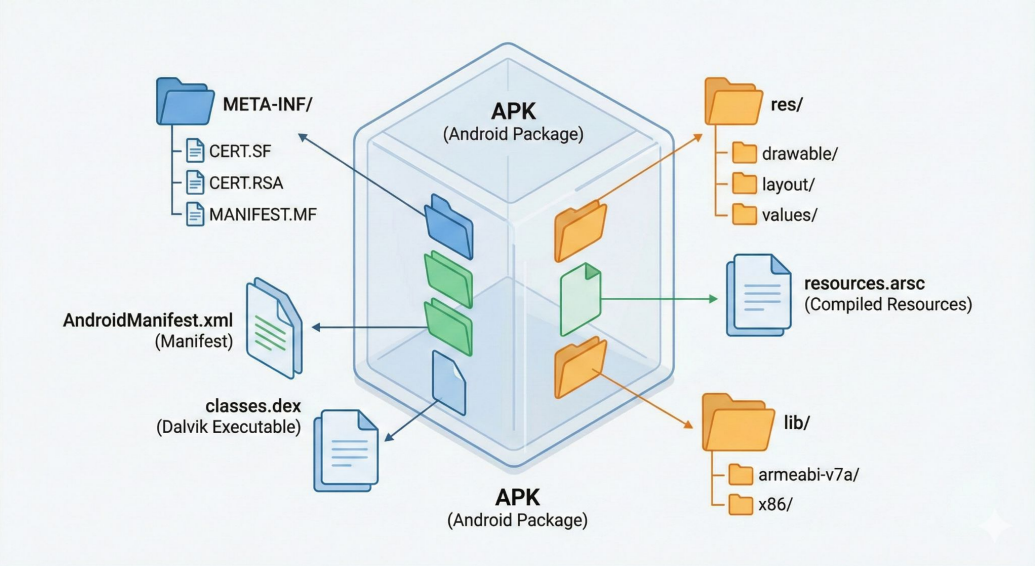
Giới thiệu

- Sự phổ biến rộng rãi của hệ điều hành Android nên mã độc di động ngày càng tinh vi hơn.
- Các phương pháp phòng thủ truyền thống dần dần bộc lộ những hạn chế đối với những mã độc chưa từng xuất hiện.
- Đã tồn tại những mô hình Máy học hỗ trợ và giải quyết những bài toán liên quan tới mã độc Android. Nhưng vẫn còn hạn chế về dữ liệu nên khó nhận ra những mã độc mới.
- Mô hình Generative Adversarial Networks (GAN) là một phương pháp mới tiếp cận và giải quyết bài toán về thiếu hụt dữ liệu.

Mục tiêu

- Sử dụng mô hình Generator để giải quyết các hạn chế của những phương pháp phòng thủ truyền thống, từ đó nâng cao năng lực bảo mật cho hệ sinh thái di động trước các mối đe dọa ngày càng gia tăng.
- Mô hình Generator cân bằng tỷ lệ phân phối giữa lớp ứng dụng an toàn và lớp mã độc để tránh thiên vị dữ liệu.
- Huấn luyện mô hình GAN đạt được độ chính xác cao cùng với những thông số đánh giá khác như Precision, Recall, F1-Score

Nội dung và Phương pháp



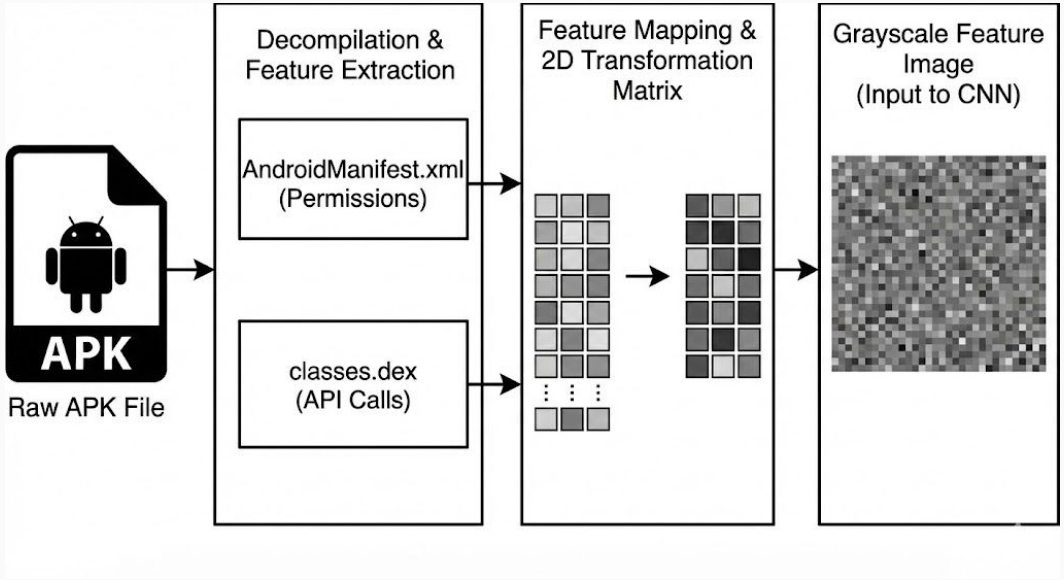
Cấu trúc của APK

Phần cốt lõi của APK là **AndroidManifest.xml** và các tệp tin thực thi **classes.dex**

AndroidManifest.xml: Chứa các quyền truy cập của ứng dụng

classes.dex: Chứa logic của ứng dụng

Nội dung và Phương pháp



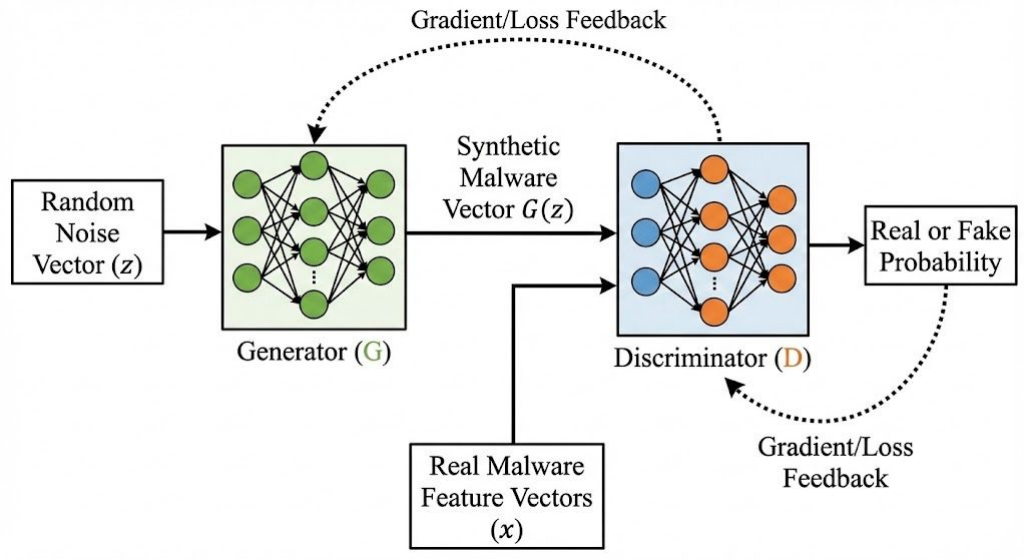
Trích xuất dữ liệu

Chuyển hoá đặc trưng (mã nhị phân) thành Graycode. Một Graycode tương ứng với một pixel trên hình ảnh.

[0,1,1,1,0,1,1,0] -> 245

Hình ảnh là dữ liệu huấn luyện cho mô hình GAN

Nội dung và Phương pháp



Hoạt động của GAN

- Generator (G) và Discriminator (D).
- vector nhiễu ngẫu nhiên (z).
- Vector đặc trưng mã độc nhân tạo (G(z)).
- Dữ liệu thật (x)

Kết quả dự kiến

- Thiết lập sự cân bằng phân phối dữ liệu nhờ mô hình Generator.
- Cải thiện các chỉ số đánh giá tiêu chuẩn bao gồm Precision, Recall và F1-Score.
- Giảm thiểu tỷ lệ tỷ lệ bỏ sót mã độc trong thời đại mã độc mới có tần suất xuất hiện liên tục.

Tài liệu tham khảo

- Nitesh V. Chawla, Kevin W. Bowyer, Lawrence O. Hall, W. Philip Kegelmeyer: SMOTE: Synthetic Minority Over-sampling Technique. J. Artif. Intell. Res. 16: 321-357 (2002)
- Ian J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron C. Courville, Yoshua Bengio: Generative Adversarial Nets. NIPS 2014: 2672-2680
- Lakshmanan Nataraj, S. Karthikeyan, Gregoire Jacob, B. S. Manjunath: Malware images: visualization and automatic classification. VizSec 2011: 4