PHÁT HIỆN MÃ ĐỘC LẨN TRÁNH DỰA TRÊN OPCODE SỬ DỤNG MẠNG NƠ-RON HỌC SÂU HỒI QUY KẾT HỢP XỬ LÝ NGÔN NGỮ TỰ NHIÊN

Trần Nguyễn Đức Huy - 230202027

Tóm tắt

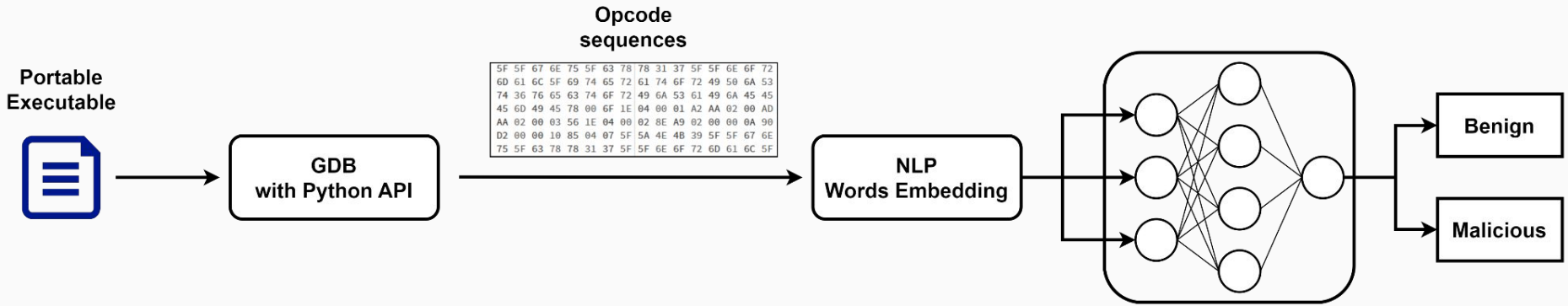
- Lớp: CS2205.MAR2024
- Link Github: https://github.com/revirven/CS2205.MAR2024
- Link YouTube video: https://youtu.be/tXH_nX5-BrU
- Ảnh + Họ và Tên: Trần Nguyễn Đức Huy
- Tổng số slides không vượt quá 10

Giới thiệu

- Công nghệ phát triển, máy tính trở thành công cụ không thể thiếu
- Mã độc ngày càng tinh vi và trở thành mối đe dọa đến người dùng
- Các giải pháp phát hiện mã độc hiện tại chưa có khả năng nhận diện các loại mã độc được áp dụng kỹ thuật lẩn tránh

Giới thiệu

Một giải pháp phát hiện mã độc lẩn tránh dựa trên opcode sử dụng mạng nơ-ron học sâu hồi quy kết hợp xử lý ngôn ngữ tự nhiên



Mục tiêu

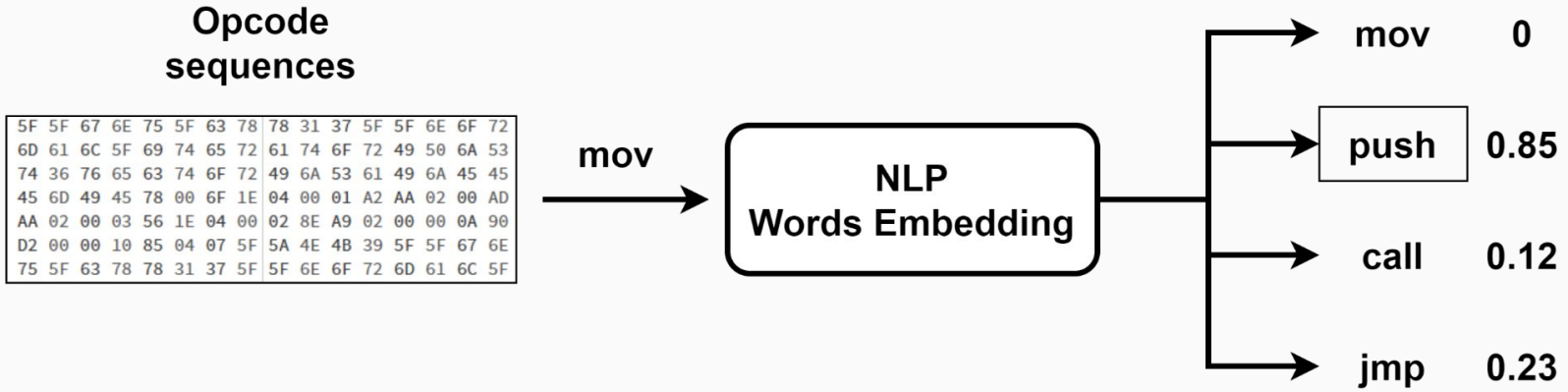
- Thu thập và xây dựng một bộ dữ liệu mã độc
- Xây dựng và huấn luyện mô hình phát hiện mã độc
- Áp dụng và đánh giá được mức độ ảnh hưởng của các kỹ thuật xử lý ngôn ngữ tự nhiên trong phân tích opcode

Nội dung và Phương pháp

- **Dataset:**
  - Thu thập và sử dụng các bộ dataset mã độc ở định dạng PE như BODMAS, EMBER,...
- **Trích xuất đặc trưng:**
  - Opcode được trích xuất từ các tệp PE trong thời gian thực thi thông qua GDB, tự động hóa sử dụng Python API của GDB
- **Tiền xử lý dữ liệu:**
  - Cân bằng tập dữ liệu bằng cách thu thập thêm mẫu hoặc sử dụng các kỹ thuật sinh dữ liệu như SMOTE, ADASYN,...

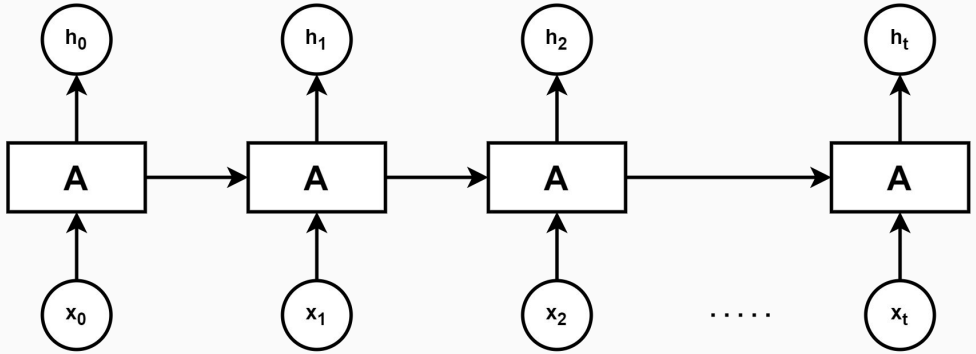
Nội dung và Phương pháp

- **Word embedding:**
  - Phân tích opcode sử dụng các kỹ thuật xử lý ngôn ngữ tự nhiên trước khi đưa vào mạng nơ-ron học sâu hồi quy
  - Nghiên cứu các mô hình Word2Vec, BERT,...



Nội dung và Phương pháp

- **Huấn luyện mạng nơ-ron học sâu hồi quy**
  - Mạng nơ-ron học sâu hồi quy có khả năng kết hợp dữ liệu của các lớp trước với dữ liệu của lớp hiện tại
  - Thử nghiệm các thuật toán học sâu hồi quy khác nhau như RNN, LSTM, GRU,...



Kết quả dự kiến

- Giải pháp đề xuất có khả năng phát hiện được các họ mã độc đa hình hay các họ mã độc được áp dụng các kỹ thuật lẩn tránh khác
- Mô hình xử lý ngôn ngữ tự nhiên có tác động tích cực đến độ chính xác của mô hình học sâu được xây dựng

Tài liệu tham khảo

[1] Mahmoud Kalash, Mrigank Rochan, Noman Mohammed, Neil D. B. Bruce, Yang Wang, Farkhund Iqbal: Malware Classification with Deep Convolutional Neural Networks. NTMS 2018: 1-5

[2] Enes Sinan Parildi, Dimitrios Hatzinakos, Yuri A. Lawryshyn:
Deep learning-aided runtime opcode-based Windows malware detection. Neural Comput. Appl. 33(18): 11963-11983 (2021)

[3] Deniz Demirci, Nazenin Sahin, Melih Sirlanci, Cengiz Acartürk:
Static Malware Detection Using Stacked BiLSTM and GPT-2. IEEE Access 10: 58488-58502 (2022)

[4] Li Yang, Junlin Liu:TuningMalconv: Malware Detection With Not Just Raw Bytes. IEEE Access 8: 140915-140922 (2020)