NGHIÊN CỨU MÔ HÌNH BỀN VỮNG CHO PHÁT HIỆN TẤN CÔNG CÓ CHỦ ĐÍCH

Trương Thị Hoàng Hảo - 240202022

Tóm tắt

- Lớp: CS2205.CH190
- Link Github của nhóm: Github
- Link YouTube video: Youtube
- Presenter: Trương Thị Hoàng Hảo
- Tổng số slides không vượt quá 10

Giới thiệu

- APT đã trở thành một mối đe dọa phức tạp và dai dẳng.
- Các hệ thống IDS truyền thống hiện đang gặp khó khăn trong việc phát hiện APT do đặc tính "slow & low" - hoạt động chậm và âm thầm.
- Đề xuất xây dựng một mô hình phát hiện APT bền vững dựa trên phân tích đồ thị truy nguyên kết hợp với các kỹ thuật machine learning/deep learning.

Mục tiêu

- Xây dựng mô hình bền vững phát hiện tấn công APT dựa trên ML/DL và PG.
- Tối ưu hóa hiệu suất của mô hình để đạt được độ chính xác cao, tỷ lệ báo động giả thấp theo thời gian thực.
- Đánh giá và kiểm chứng hiệu suất của mô hình trên các tập dữ liệu chuẩn.

Nội dung và Phương pháp

1. Nội dung 1: Tìm hiểu về cách xử lý dữ liệu PG

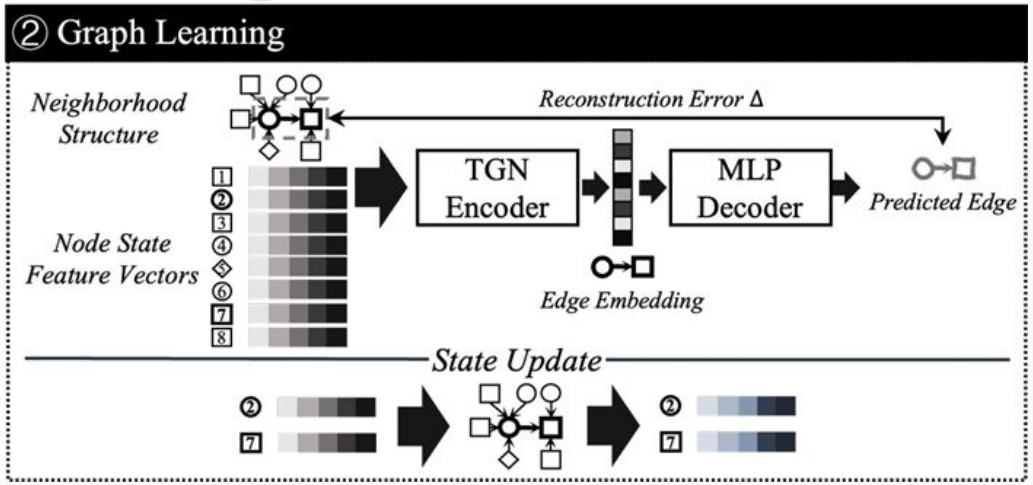
- Nghiên cứu các tập dữ liệu điển hình như DARPA TC và OpTC.
- Nghiên cứu các tài liệu khoa học liên quan và triển khai các phương pháp biến đổi dữ liệu thô thành PG.

2. Nội dung 2: Tìm hiểu về thuật toán gom nhóm và cách biểu diễn đồ thị

- Tìm hiểu và thử nghiệm thuật toán gom nhóm, điển hình là Louvain.
- Tìm hiểu và so sánh các cách biểu diễn đồ thị, bao gồm: node embedding, edge embedding, subgraph embedding, ...

Nội dung và Phương pháp

3. Nội dung 3: Tìm hiểu về các mô hình ML/DL trong nghiên cứu [2]



Nội dung và Phương pháp

4. Nội dung 4: Xây dựng mô hình phát hiện tấn công APT

Dựa vào những kiến thức tìm hiểu được để xây dựng mô hình đa lớp phát hiện tấn công APT theo thời gian thực, có tính bền vững trước các loại tấn công phức tạp.

5. Nội dung 5: Thực nghiệm và đánh giá kết quả

- Đánh giá hiệu năng, độ hiệu quả của mô hình đã xây dựng.
- Tìm ra những điểm yếu và hướng phát triển trong tương lai.

Nội dung và Phương pháp

2. Nội dung 2: Tìm hiểu về thuật toán gom nhóm và cách biểu diễn đồ thị

- Tìm hiểu và thử nghiệm thuật toán gom nhóm, điển hình là Louvain.
- Tìm hiểu và so sánh các cách biểu diễn đồ thị, bao gồm: node embedding, edge embedding, subgraph embedding, ...

Kết quả dự kiến

- Xây dựng thành công mô hình phát hiện tấn công APT bền vững bằng cách áp dụng ML/DL và PG.
- Tài liệu đánh giá tính hiệu quả, bền vững của mô hình đề xuất.

Tài liệu tham khảo

[1] Zhengqiu Weng, Weinuo Zhang, Tiantian Zhu, Zhenhao Dou, Haofei Sun, Zhanxiang Ye, and Ye Tian. RT-APT: A real-time APT anomaly detection method for large-scale provenance graph. *J. Netw. Comput. Appl.*, 233:104036, 2025.

[2] Zijun Cheng, Qiu Jian Lv, Jinyuan Liang, Yan Wang, Degang Sun, Thomas Pasquier, and Xueyuan Han. Kairos: Practical intrusion detection and investigation using whole-system provenance. In *IEEE Symposium on Security and Privacy (SP)*, pages 3533–3551. IEEE, 2024.