NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE
School of Computer Science and Engineering
College of Engineering

Provenance Graph Generation for Intrusion Detection

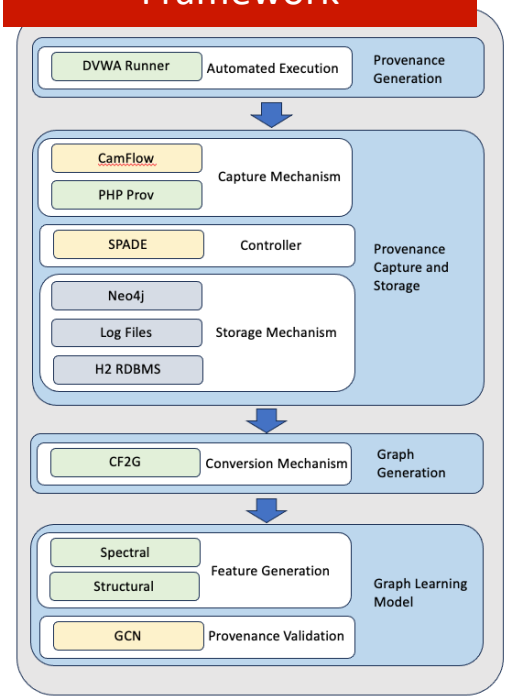
Simulating Scenarios for Graph Convolutional Network Classification

Student: LIM ZIYI JANESSE Supervisor: A/P KE YIPING KELLY

Project Objectives:

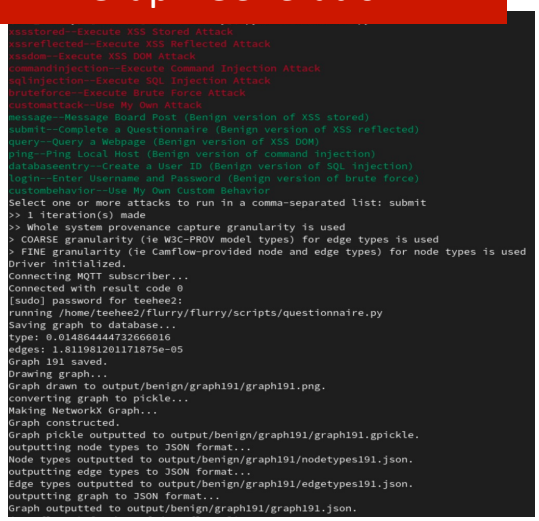
In this study, our objective is to validate the effectiveness of provenance graphs in intrusion detection by generating and analysing benign and malicious user scenarios. Leveraging the CamFlow provenance capture system and the Flurry framework, we will simulate diverse intrusion scenarios and generate authentic provenance data. Our aim is to evaluate state-of-the-art graph-based models for intrusion detection using performance assessment metrics such as classification accuracy, precision recall and f1-score. Through this investigation, we aim to contribute to the advancement of intrusion detection methodologies and enhance our understanding of provenance-based defense mechanisms.

Framework

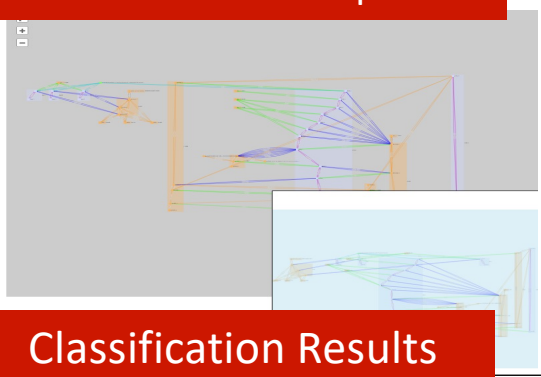


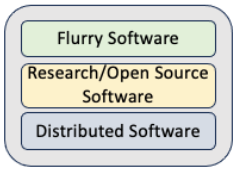
As adapted from Flurry's framework [1]

Graph Generation



Provenance Graph





Legend

[1] M. Kapoor, J. Melton, M. Ridenhour, M. Sriram, T. Moyer, and S. Krishnan, 'Flurry: a Fast Framework for Reproducible Multi-layered Provenance Graph Representation Learning'. arXiv, Mar. 05, 2022. Available: http://arxiv.org/abs/2203.02744

Classification Results

Metric	Accuracy	Precision	Recall	F1-Score
Malicious Executions	67.010.15	70.030.25	76.341.25	73.221.63