[Demo] Edge-based IoT Intrusion Detection

Yimin Zhang[1,2], Barikisu Asulba[1,2], Nuno Schumacher[1,2], Mário Sousa[1,2], Pedro Souto[1,2], Luis Almeida[1,2*], Pedro Santos[1,3], Luis Gomes[4], Nuno Martins[4], Joana Sousa[4]

[1]Res. Center in Real-Time Emb. Comp. Systems (CISTER), Portugal.
[2*]Faculdade de Engenharia, Universidade do Porto (FEUP), Portugal.
[3]Instituto Superior de Engenharia do Porto (ISEP), Portugal.
[4]NOS Inovação, Lisboa, Portugal.

*Corresponding author(s). E-mail(s): lda@fe.up.pt;

Abstract

This demonstration showcases an IoT-focused intrusion detection system based on Machine-Learning (ML) models running at the edge, deployed both on a regular computer and on the router of an Internet Service Provider (ISP). The ML intrusion detection pipeline was designed and deployed with Node-RED, a low-code and event-driven framework, within the ITEA MIRAI project.

Keywords: intrusion detection, IoT, ML, embedded systems, edge computing.

1 Introduction

An ideal household cyber-security protection system should handle novel network traffic types and adapt to diverse legitimate Internet usage patterns across different households and including IoT devices. Machine Learning (ML) enables the learning and recognition of legitimate network traffic patterns, thus detecting anomalous patterns that may indicate attacks [1]. The ITEA MIRAI project[1] aims at deploying industry ML applications in the edge. It includes a use case for securing IoT home ecosystems in which we explore edge-computing to detect intrusions locally, avoiding cloud-based approaches that would imply sending traffic features over public networks, further widening the exposure surface. This demonstrator showcases the intrusion detection system using publicly available traffic datasets.

[1] https://project-mirai.eu/

2 Demonstrating the intrusion detection pipeline

To improve the reconfigurability of our ML inference pipeline we selected Node-RED [2], a low-code development and deployment framework with high modularity (Fig. 1).

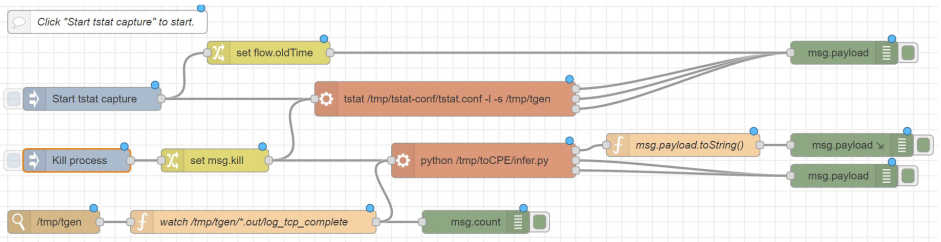
Click "Start tstat capture" to start.
set flow.oldTime
msg.payload
Start tstat capture
tstat /tmp/tstat-conf/tstat.conf -l -s /tmp/tgen
msg.payload.toString()
msg.payload
Kill process
set msg.kill
python /tmp/toCPE/infer.py
msg.payload
/tmp/tgen
watch /tmp/tgen/*.out/log_tcp_complete
msg.count

Fig. 1: ML inference pipeline instantiated as a Node-RED flow.

There are two major components in our solution, one is the `tsat` tool available in Linux that extracts features from the incoming traffic and the other is the ML model implemented in Python. We used models from the One-Class type that are suitable to anomaly detection. These models are trained exclusively with data of one class, in this case normal benign traffic, and detect data that falls outside, thus potentially malicious. Though we have used several models of this class [3], this demonstrator shows results of the Elliptic Envelope model, only. Then we inject traffic from publicly available datasets and submit them to our ML pipeline, which shows an accuracy above 80%. This can be further improved by combining different models as proposed in [3]. The resource usage and execution time of the ML pipeline deployed with Node-RED on the router of an ISP provider is shown in [2]. The Node-RED framework together with needed Python libraries take less than 60MB of the router memory and the execution time of the ML pipeline takes under 27ms, while the features extraction time by `tstat` may add a few seconds depending on the specific traffic flow.

Acknowledgments. This work was partially supported by National Funds through FCT/MCTES (Portuguese Foundation for Science and Technology), within the CISTER Research Unit (UIDB/04234/2020) and ANI (Portuguese National Innovation Agency) within the COMPETE 2020 program under the PT2020 Partnership Agreement, and through the European Regional Development Fund (ERDF) within project grant 69522, POCI-01-0247-FEDER-069522 (MIRAI).

References

[1] Alkasassbeh, M., Al-Haj Baddar, S.: Intrusion detection systems: A state-of-the-art taxonomy and survey. Arabian J. for Science and Eng. **48**, 10021–10064 (2023)

[2] Zhang, Y., Asulba, B., Schumacher, N., Sousa, M., Souto, P., Almeida, L., Santos, P., Martins, N., Sousa, J.: Implementing and Deploying an ML Pipeline for IoT Intrusion Detection with Node-RED. RAGE 2023 (in ACM CPS-IoT Week) (2023)

[3] Schumacher, N.: Anomaly Detection Models for Cloud-edge Intrusion Detection in Customer Networks. Universidade do Porto, Master Thesis (2022)