Contribution ID: **186** Type: **Paper presentation**

Metadata-based Network Traffic Analysis Using Zeek

Thursday 18 September 2025 12:25 (15 minutes)

Networks usually face the challenges of high traffic volume and diverse user behaviours, which makes analyzing and preventing security incidents particularly difficult. Another major drawback is that traffic is often encrypted, so the data you can analyse is very limited. This paper presents an approach to network monitoring tooling, using Zeek for inspection on encrypted traffic. The system is designed to analyse metadata, flow characteristics and other anomalies. To increase detection rate and contextual awareness, the deployment integrates with Malware Information Sharing Platform (MISP) for real-time threat intelligence correlation, and OpenSearch for scalable indexing, querying, and integrating with other logs from the same network. This setup allows detection of suspicious activity, threat hunting and intrusion prevention across the entire infrastructure. The system architecture is modular and scalable, allowing it to apply different security policies to the intrusion detection software and adjust the configuration to suit traffic patterns. We discuss the architectural design, performance, testing, and practical challenges of monitoring encrypted traffic on high volume network traffic.

Authors: JUMAREA, Stefan Dorin (National University of Science and Technology POLITEHNICA Bucharest); MIHAI, Darius (Universitatea Națională de Știință și Tehnologie POLITEHNICA București); MIHAILESCU, Maria-Elena (National University of Science and Technology POLITEHNICA Bucharest, Romania); OCANOAIA, Andreia-Irina (National University of Science and Technology POLITEHNICA Bucharest); Mr CARABAS, Mihai (National University of Science and Technology POLITEHNICA Bucharest); Mr DAGILIS, Lukas Vytautas (NRD Cyber Security); GRAMA, Andreea (Revel Business Group)

Presenter: JUMAREA, Stefan Dorin (National University of Science and Technology POLITEHNICA Bucharest)

Session Classification: Cloud Computing and Network Virtualisation

Track Classification: Network Security