LITHUANIAN COMPUTER SOCIETY
VILNIUS UNIVERSITY, INSTITUTE OF DATA SCIENCE AND DIGITAL TECHNOLOGIES
LITHUANIAN ACADEMY OF SCIENCES

16th Conference on

DATA ANALYSIS METHODS
for Software Systems

November 27–29, 2025

Druskininkai, Lithuania, Hotel "Europa Royale"
https://www.mii.lt/DAMSS

VILNIUS UNIVERSITY PRESS
Vilnius, 2025

Contacts:

Dr. Jolita Bernatavičienė
jolita.bernataviciene@mif.vu.lt
Prof. Olga Kurasova
olga.kurasova@mif.vu.lt
Tel. (+370 5) 2109 315

https://doi.org/10.15388/DAMSS.16.2025
ISBN 978-609-07-1200-9 (digital PDF)

Modelling of Cyber Security Attacks in Large Asynchronous Network Flows

Virgilijus Krinickij, Linas Bukauskas

Cyber Security Laboratory
Institute of Computer Science
Faculty of Mathematics and Informatics
Vilnius University

virgilijus.krinickij@mif.vu.lt

Cyber security is one of the most versatile subfields today. For modelling possible attacks on organisations network, professionals need to develop a system that would be capable of generating asynchronous network flows. These network flows would be used for the assessment of possible cyber events in the future to prevent attackers from breaching the organization. This work presents a practical, production-minded architecture for distributed network-flow collection on Linux hosts. The created system couples a message-driven control plane and enables on-demand capture, dynamic filter updates, and resilient return-path streaming of packet artifacts for storage and analysis. On endpoints, a Python client built on Scapy performs interface-level sniffing and applies BPF filters supplied asynchronously via RabbitMQ. Filters are created using predefined records in a database structure that are pushed as queue messages from the RabbitMQ broker server to the client machine. The client machine can take multiple instances of the network filter. The agent in the client machine, based on the filter, produces captured packets, which in turn are serialized and returned over callback queues, where the RabbitMQ server component persists them to PCAP files and logs event metadata. Also, time-based anomaly injection and cyberattack templates are supported for testing and experiments. The asynchronous aspect of the system comes from a predefined network configuration, which is a part of the overall system design. We assume that a predefined network configuration is a set of networks in a laboratory setup where we simulate real-life networks with different configurations and at different times. For this, we use Proxmox, a powerful open-source virtualization

platform. Operationally, Proxmox hosts provides virtual machine and Linux container (LXC) placement, while an Ansible playbook codifies provisioning for system automation. System automation is needed so that there would be less downtime in different environments where the system would be needed. For future cyberattack assessment in produced PCAP files we will use different algorithms like Dynamic Time Warping (DTW), windowed DTW, Needleman-Wunch, Smith Waterman. A possible machine learning functionality can also be added for high-throughput live data flow analysis in the RabbitMQ server machine. We also discuss web-exposed upload vulnerabilities, emphasizing why executable payloads must never be writeable in web-served paths and how defense-in-depth (MIME/extension whitelists, server-side execution blocks) prevents remote code execution. Altogether, the solution demonstrates a portable, automatable pipeline for remote capture and adaptive telemetry at scale, balancing performance, operability, and security.