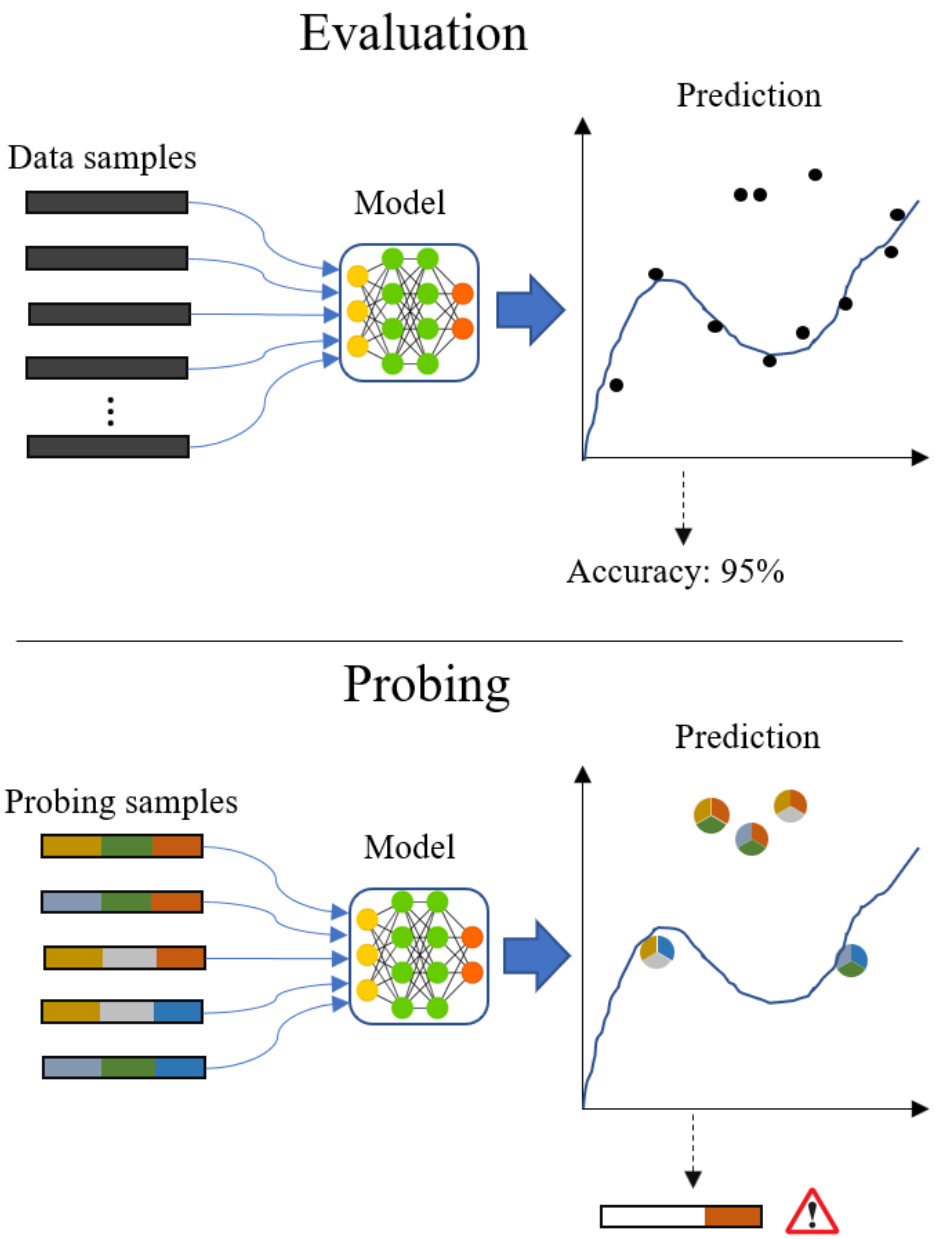
DetGen

Aim:

- Provide controllable traffic data from different settings
- Ground truth labels on what the traffic *micro-structures* "represents"
- Reproducible

Why:

- Originally to build software models
- Now to understand and explore models

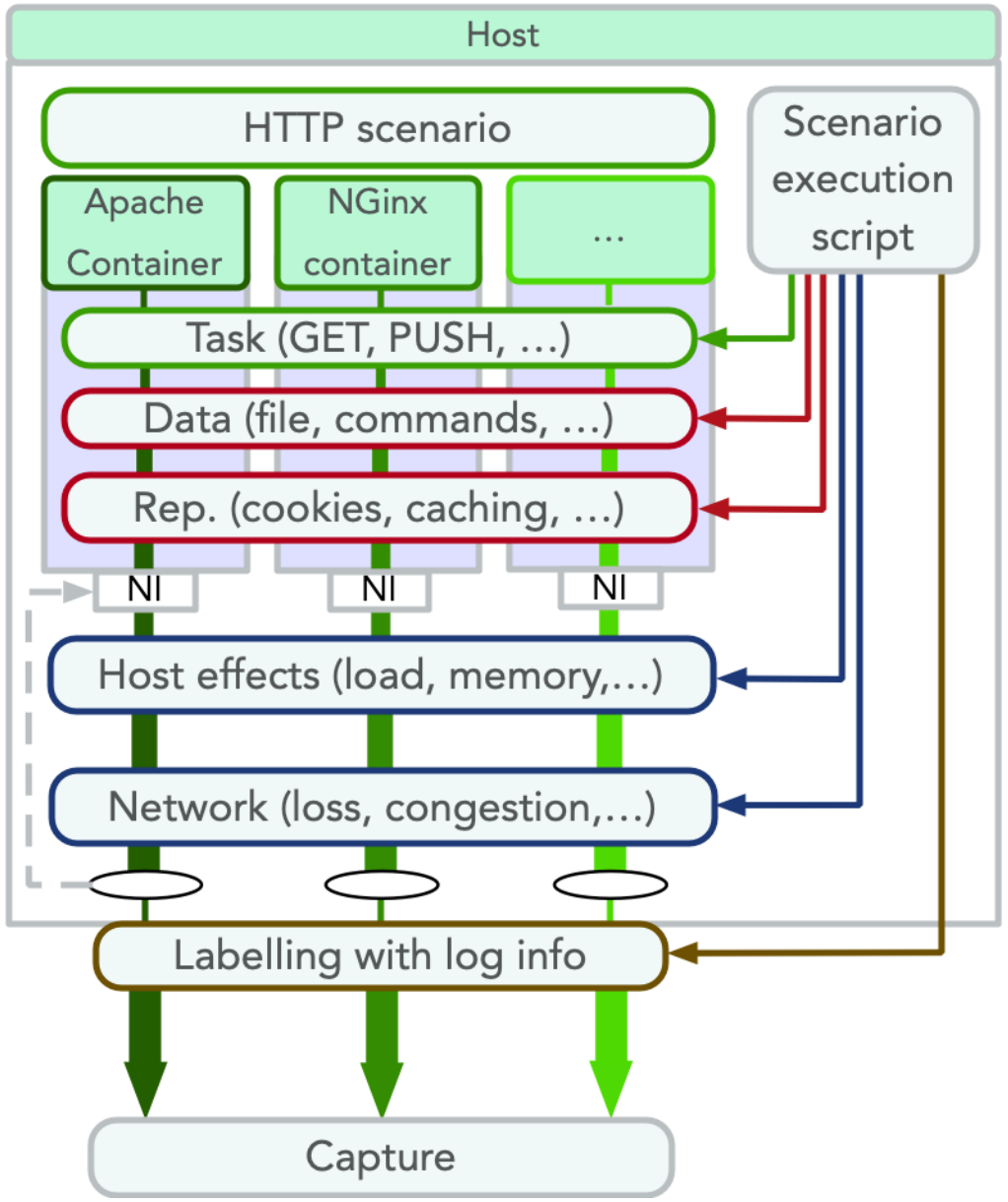


Design

- Containerisation
  - Traffic separation
  - Isolation from other processes
  - Reproducible and easy to modify setting

- Scripted scenarios generate traffic
- Execution script controls different settings
- PCAP-file with labels after each run

- 26 scenarios so far



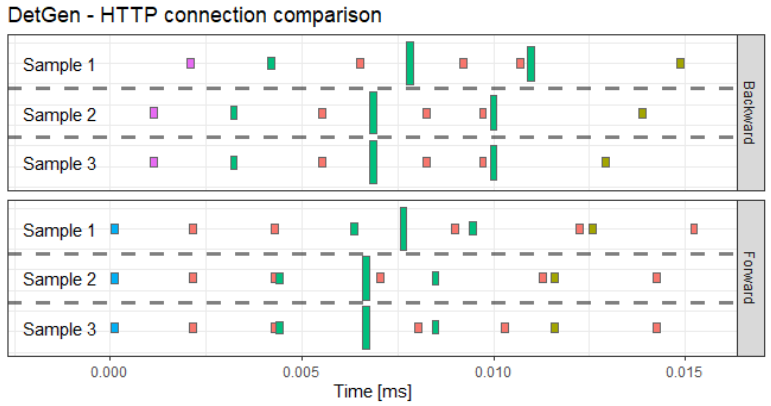
Publications

2.5 papers so far:

- DetGen for ML at DYNAMICS workshop
  - Some experiments to verify ML-usefulness
- Probing demonstrations submitted to WTMC workshop
- Usage of stepping-stone data for NSS-paper

Materials not used:

- Description of framework
  - Focus on control over structures
- Determinism experiments



- Diversity experiments
  - Drawing comparison to other NIDS datasets

Plan

Prepare paper for SecureComm

- Deadline: 15th March

Checklist for strong contribution:

- Make repo more usable for others
  - Potentially graphical interface?

- Generate exemplary dataset(s)
  - What should this data provide?
    - Demonstrate probing capabilities?
    - Demonstrate determinism/reproducibility?

- Focus on how we can build a model that is better understandable using these microstructures
- Rob: Multi-stage
- Invite Michael on call, check on why they didn't use detgen