ntop Webinar 2022

nDPId

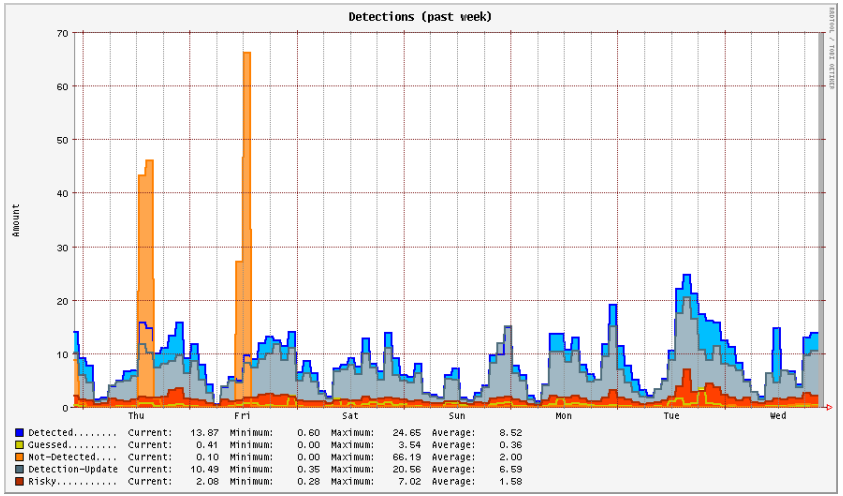
https://github.com/utoni/nDPId

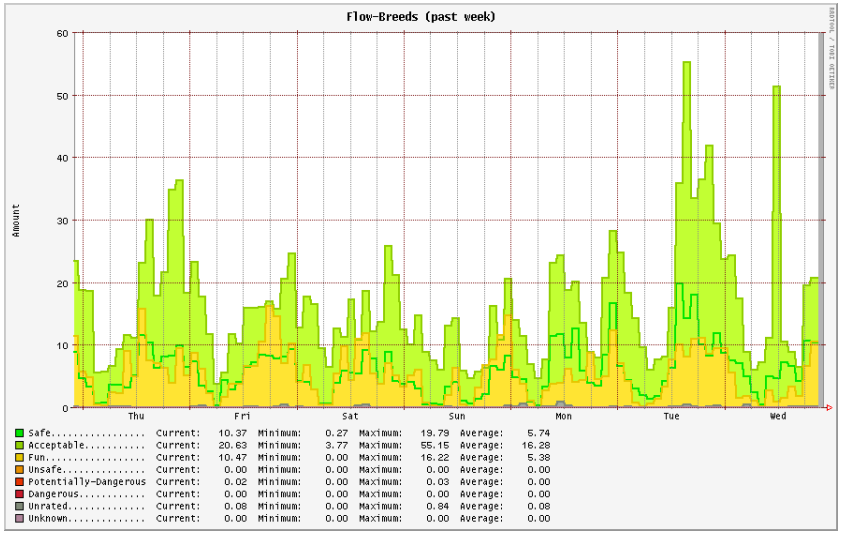
Toni Uhlig <toni@impl.cc>

What is nDPId?

- collection of several daemons and tools to capture, process, classify and visualize network traffic
  - main daemons: nDPId, nDPIsrvd
  - tools / examples / user applications:
    - collectd wrapper, raw packet dumper, pretty flow printer, ML feature extractor, ML flow classification using sklearn, ...

What is nDPId?





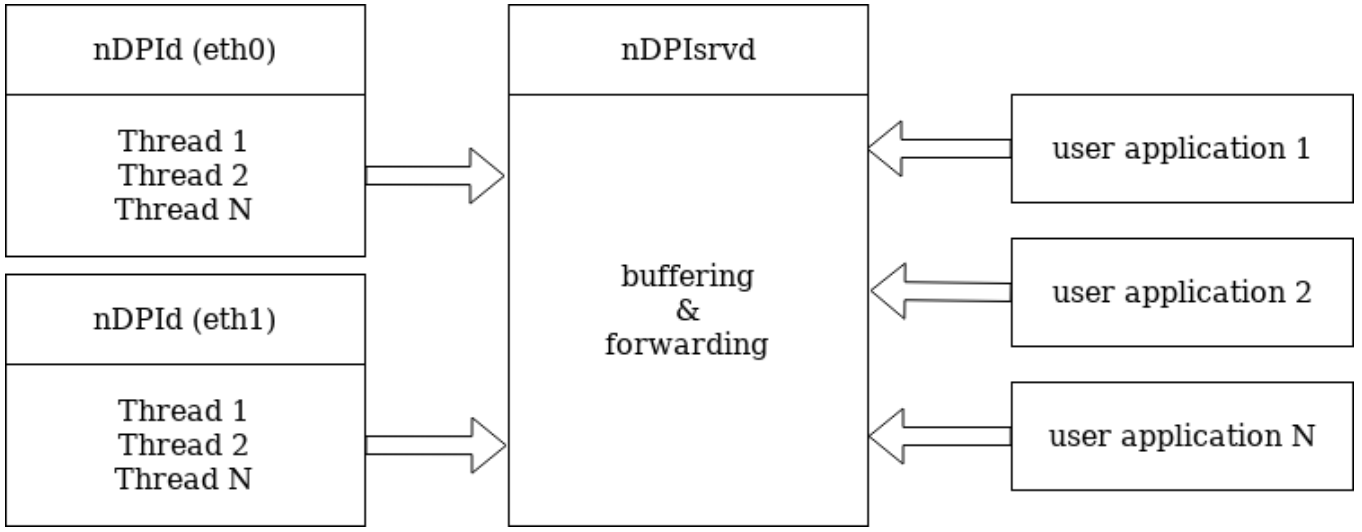
History of nDPId

- initially started as simple integration example for libnDPI (2020)
  - ndpiReader offers a wide range of functionality
  - high complexity and memory usage
    - just an example to show some libnDPI features
- evolved into a daemon / tool suite

nDPId Goals

- obligatory flow classification with libnDPI
- generate and send JSON events to other applications
- low memory footprint
- minimal dependencies to other libraries
- high scalability

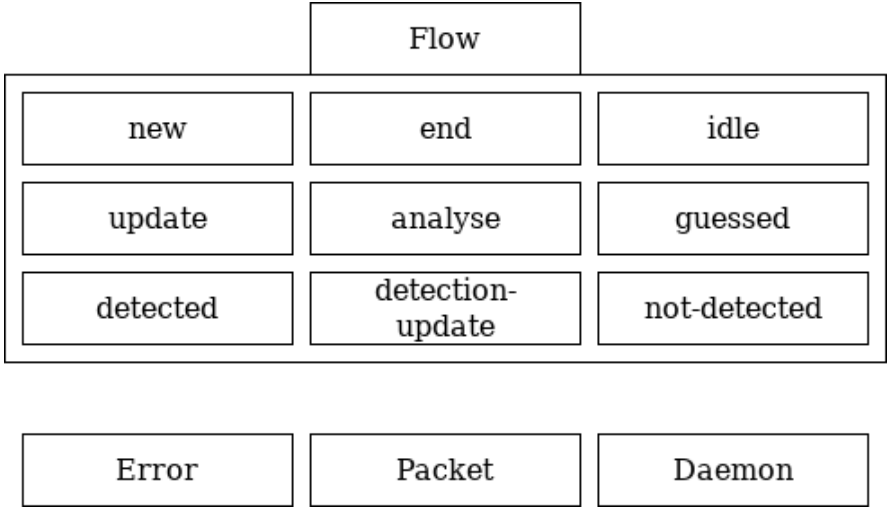
nDPId Architecture



nDPId message format

- concatenation of the message length and JSON string
- example: 00016{'key':'value'}\n

nDPId events



Plans for 2023 (nDPId)

- Android support
- port to BSD/OSX
- GnuTLS / “push” support for nDPIsrvd
- other ML/DL approaches for protocol classification and anomaly/malicious traffic detection
  - Keras based Autoencoder (work-in-progress)
- detect false-positives using ML

Plans for 2023 (libnDPI)

- generic packet reassemble engine for stream based protocols e.g. TCP/QUIC
  - work-in-progress
  - usable for all layer 7 protocol dissectors
- move code from ndpiReader to the core library
  - datalink processing (?)
  - layer 3 / layer 4 tunnel detection
- reduce false-positives for certain protocol dissectors

Special Thanks

- Ivan Nardi
- Damiano Verzulli from GARRLab
- Luca Deri and the ntop team