

# nDPI: what's new, what's next and what is it useful for?

Ivan Nardi

# Who am I?

- Ivan Nardi, @ AI2M
  - lawful interception, investigation analysis, big data retention
  - voice/IP metadata collection, processing and reporting
  - network probes and DPI
  
- [ivan@ai2m.eu](mailto:ivan@ai2m.eu)

# nDPI: what is it?

- An open-source library providing:
  - deep packet inspection engine for network visibility: protocol classification, metadata extraction, flow risks computation
    - basic blocks for a cyber-security application
  - algorithms for data analysis:
    - data forecasting and anomaly detection
    - clustering and similarity evaluation
    - (sub-)string searching and IP matching
    - probabilistic data structures: bloom filters, cardinality estimation

# nDPI: some statistics

- In the last year (i.e. from ntopconf22)
  - 24 contributors
  - ~600 commits

# nDPI: what is it useful for?

- Protocol classification and statistics
  - small ISP: statistics about Youtube/Netflix traffic to optimize peering
- Firewall: block/allow some kind of traffic
  - with subscriber info, block/allow rules per user
  - zero-rating applications (by ISPs)
- Cybersecurity applications
- Bandwidth control & QoS

# nDPI: what is it useful for?

- Block of (only) BitTorrent traffic on a VPN free plan
- Traffic control on enterprise VPNs
- Active honeypot
- Algorithms: detect performance regressions via statistical anomaly detection
  - <https://netflixtechblog.com/fixing-performance-regressions-before-they-happen-eab2602b86fe>

# nDPI: what's new

- Usual, boring stuff:
  - be sure that old stuff is still working...
  - new flow risks and ~50 new protocols: some VPNs, some games, few streaming services...
  - better performances, less resources, better testing
  - better internal algorithms
  - add some general statistics: Patricia tree, automata, LRU cache...
- Some documentation skeletons

# nDPI: what's new

- Better identification of VoIP/RTP traffic, even when it is explicitly blocked:
  - Zoom classification
  - RTP stream type (audio, video, screen sharing)
- More algorithms: bloom filter, count-min Sketch, popcount



# nDPI: what's new

- Better custom rules (support for custom BPF protocol definition using nBPF)
- Add an heuristic to detect fully encrypted flows
- Preliminary work to handle ECH
- Detection of (illegal) gambling sites

# nDPI: fuzzing support

- What is fuzzing? This bash one liner but fancier:
  - `while 1; do ./a.out < /dev/urandom & done`
- oss-fuzz integration started 4 years ago

# nDPI: fuzzing support

## Fuzzing Introspection of OSS-Fuzz projects

Fuzz Introspector

Suggest ideas

Report issues

Show  entries

Search:

| Project name         | Language | Fuzz target count | Runtime code coverage | Total lines |
|----------------------|----------|-------------------|-----------------------|-------------|
| go-containerregistry | go       | 1                 | 98.75                 | 160         |
| evo-inflector        | java     | 1                 | 98.50                 | 133         |
| faad2                | c        | 5                 | 97.49                 | 12185       |
| md4c                 | c        | 1                 | 97.39                 | 4290        |
| tailscale            | go       | 1                 | 96.73                 | 153         |
| uint256              | go       | 2                 | 96.62                 | 1686        |
| jsonparser           | go       | 14                | 96.38                 | 773         |
| cgif                 | c        | 1                 | 96.19                 | 919         |
| gonids               | go       | 1                 | 96.08                 | 1021        |
| nats                 | go       | 2                 | 95.91                 | 709         |
| cppitertools         | c++      | 1                 | 95.51                 | 401         |
| h3                   | c        | 20                | 94.88                 | 3868        |
| ndpi                 | c++      | 27                | 94.85                 | 39480       |
| jbig2dec             | c++      | 1                 | 93.48                 | 5657        |
| pcre2                | c++      | 1                 | 93.48                 | 16202       |

# nDPI: whats' next

- Usual, boring stuff: more protocols, better performances, more flow risks, more configuration options, better multi-core support...
- Significant improvements on BitTorrent, STUN (i.e. VoIP apps) and VPN traffic
- A new algorithm to detect DGA domains?
- Better handling of asymmetric traffic