A Formally Verified NAT Stack


Solal Pirelli


Arseniy Zaostrovnykh


Luis Pedrosa

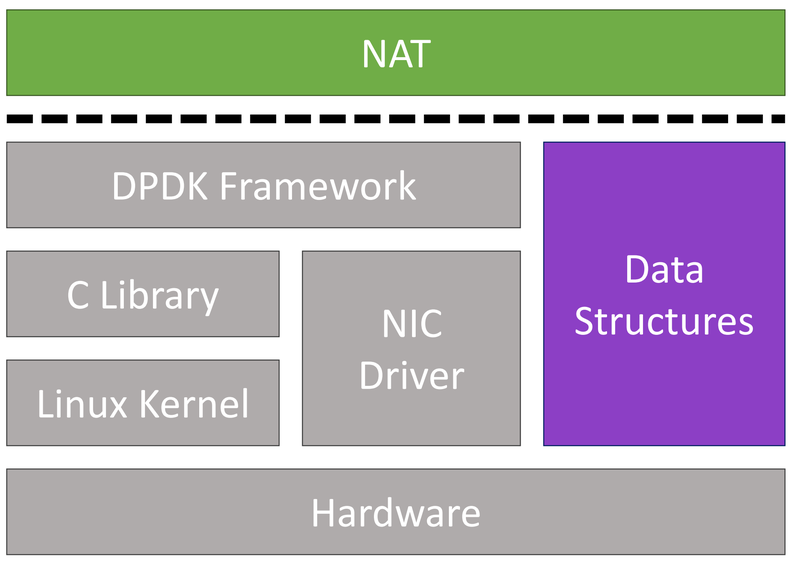

Katerina Argyraki

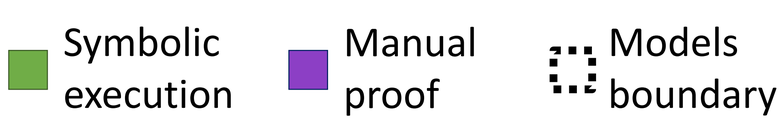

George Candea

Verified NAT

Symbolically execute NAT
Manually prove data structures
Model DPDK + driver

× Unverified components
× DPDK & driver are immature





This Work

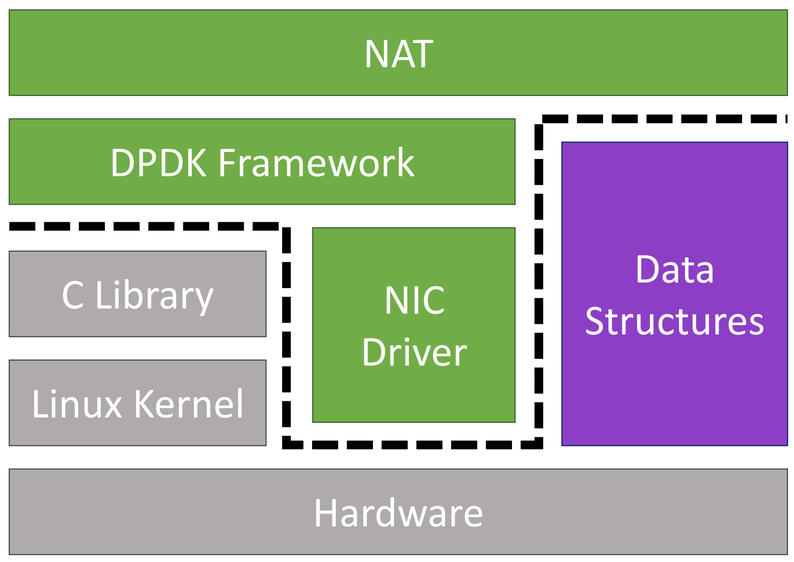
Insight
DPDK & driver are *large*, but not *complex*

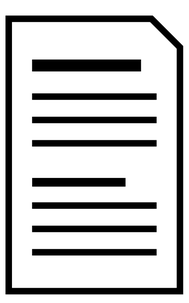
Lower-level models
C library
Hardware
- Registers
- DMA
- I^2C, SFP, …

Verified Stack

Symb. exec. NAT, DPDK, driver

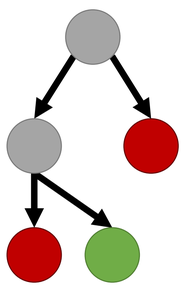
✓ More verified components
✓ Unverified code is mature





API Contracts
Low-level models
Based on specs

\+



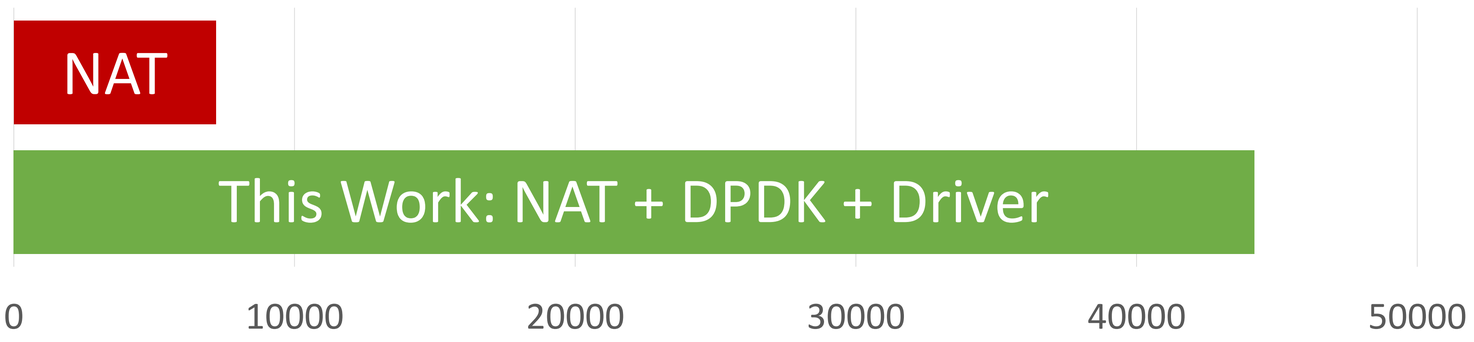
Symbolic Execution
Explore all paths
Enforce contracts

= **Correctness**

Findings

API misuses
Incorrect semantics
Synchronization errors
Non-existent registers

Covered Instructions



ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

DSLAB

Network Architecture Laboratory