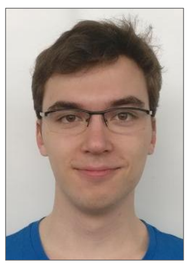
Vigor: Push-Button Verification of Software NFs



Arseniy Zaostrovnykh, Solal Pirelli, Luis Pedrosa, Rishabh Iyer, Katerina Argyraki, George Candea

Context:

- HW networking: reliable but rigid
- SW networking: flexible but flakey

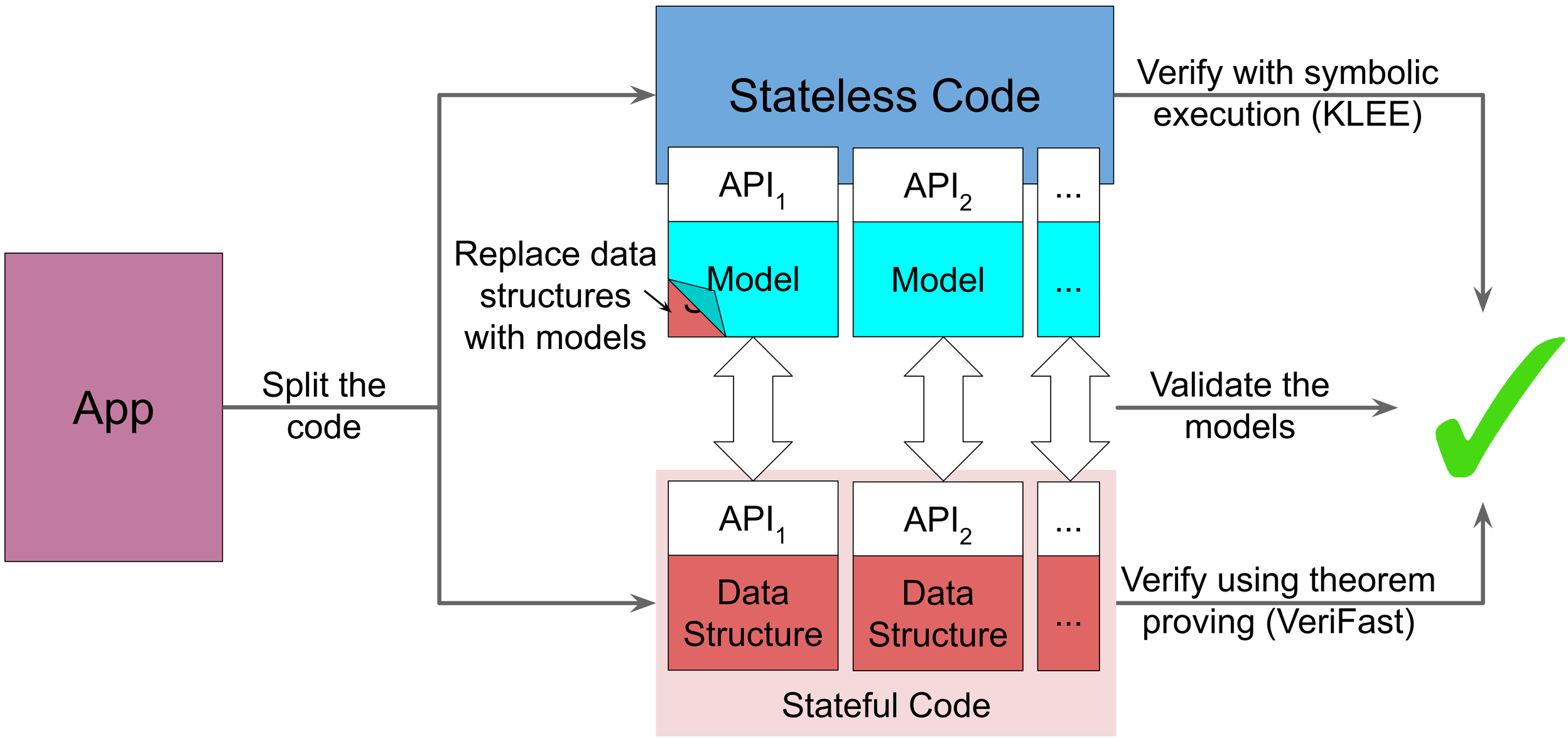
Problem:

Verification tools drawbacks:

- Too much development overhead (e.g. theorem proving) OR
- No reasoning about semantics (e.g. symbolic execution)

Insight:

- Network applications usually have clearly isolated, well-defined state
- Only some small stateful pieces of code are hard to automatically verify



We are building stateful NFs (NAT[1], Bridge, Firewall, DMZ) that are:

- Formally proven correct, secure, memory safe, crash-free
- Fast: 2x higher throughput, 3x lower latency than Linux NAT

The approach has proven to:

- Embrace framework (DPDK) code (ask Solal)
- Generalize to other languages - P4, Rust
- Support performance analysis (see Rishabh's poster)

[1] Zaostrovnykh, A., Pirelli, S., Pedrosa, L., Argyraki, K., & Candea, G. *A Formally Verified NAT*. ACM SIGCOMM 2017

DSLAB

Network Architecture Laboratory