Vigor: Trusted Software Networking

‡ DSLAB

† NAL





Arseniy Zaostrovnykh†‡, Solal Pirelli‡, Luis Pedrosa†, Katerina Argyraki†, George Candea‡

Context:

- HW networking: reliable but rigid
- SW networking: flexible but flakey
  - ❖ Mirai botnet took over >1,000,000 network devices[1]
  - ❖ Two software bugs took entire Google cloud down[2]

Problem:

Verification tools:

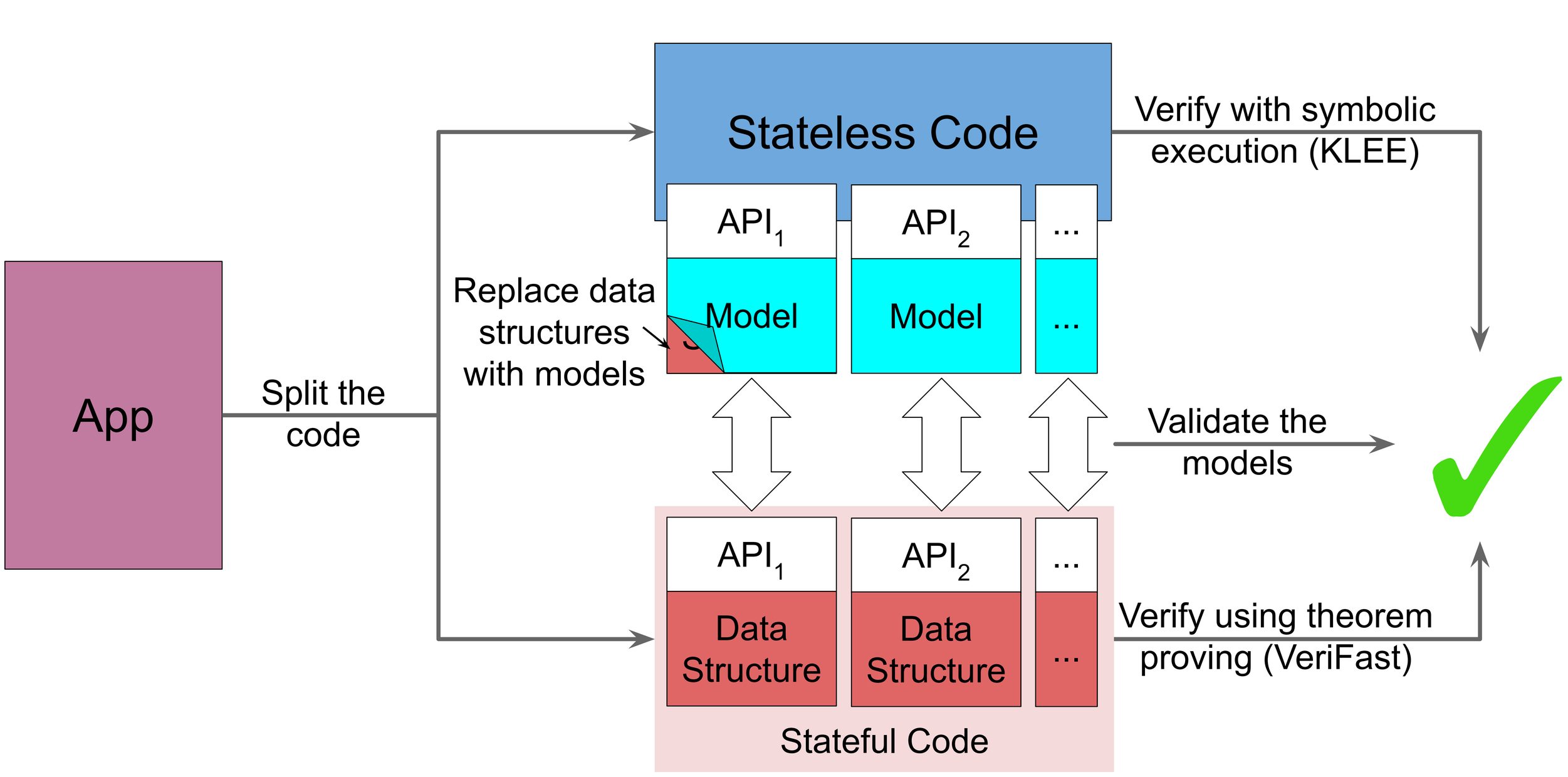
- Too much development overhead (e.g. theorem proving) OR
- No reasoning about semantics (e.g. symbolic execution)

We need a new approach that:

- Is easy to apply AND
- Supports powerful semantics

Insight:

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



We built a NAT box that is:

- Formally proven correct (= RFC3022), secure, memory safe, crash-free
- Fast: 2x higher throughput, 3x lower latency than Linux NAT

1 http://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained/
2 https://status.cloud.google.com/incident/compute/16007