Formally Verified Sandboxing for Packet-Processing Programs

Track I Award 2019302
srinivas.narayana@cs.rutgers.edu
santosh.nagarakatte@cs.rutgers.edu

Srinivas Narayana & Santosh Nagarakatte

RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

Context & Challenge:

* Flexible, CPU-efficient packet processing with eBPF kernel extensions widely deployed

* Static safety verification before loading into the kernel

* In-kernel verifier has bugs: privilege escalation, DoS

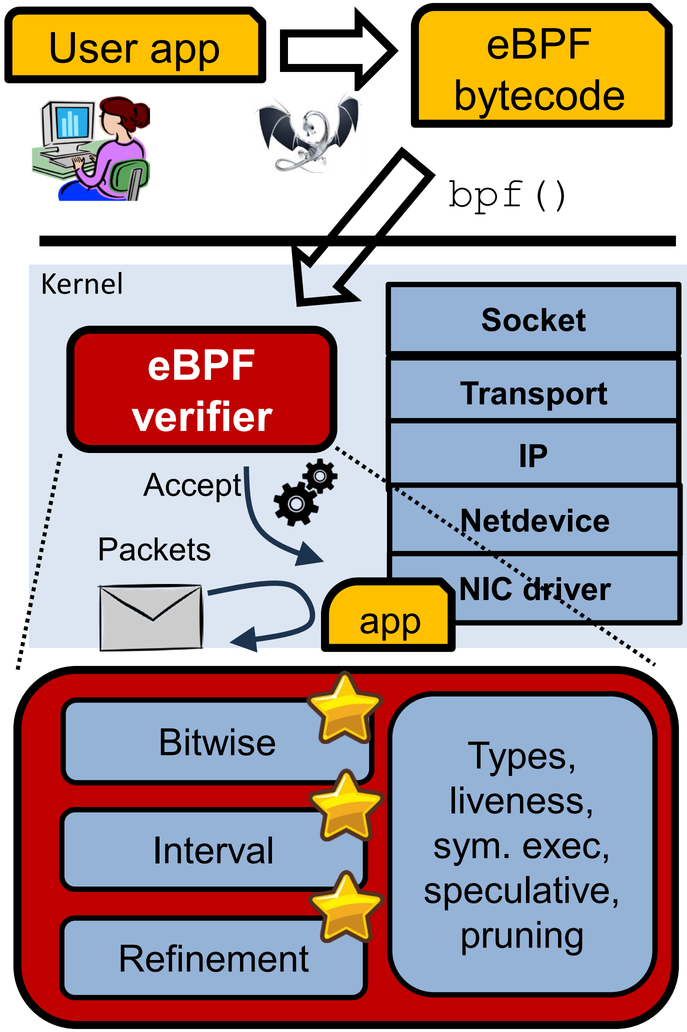
Solution:

* Formalize eBPF verification as abstract interpretation

* New sound & precise bitwise operations (CGO22)

* One-shot verification of cross-domain operators (CAV23)

* Modular verification (SAS24)



Scientific Impact:

* Novel abstract operators with proofs of soundness and precision

* Approaches for one-shot and modular verification of systems

* Generating formal models of kernel software

Broader Impact and Broader Participation:

* Three upstreamed contributions to mainline Linux kernel; 2 LPC talks

* Linux eBPF verifier CI; actively used by kernel developers

* Training 2 grad students and several undergrads