2024 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW) | 979-8-3503-6460-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/IPDPSW63119.2024.00053

Multi-core Multi-rule VeBPF Firewall for Secure FPGA IoT Device Deployments

Zaid Tahir Sahan Bandara Martin Herbordt
CAAD Lab, ECE Department, Boston University, USA. {zaidt|sahanb|herbordt}@bu.edu

I. Introduction and Motivation

FPGAs are often deployed in IoT devices: sensor technology is advancing rapidly and microcontrollers may be unable to handle the needed throughput. But with their connections to the internet and only basic system support, IoT devices may be easy targets of cyberattacks. Current FPGA-based SmartNIC defenses against cyberattacks, however, are mostly applicable in cloud deployments. In order to mitigate cyberattacks on resource-limited IoT devices, we have developed a multi-core multi-rule VeBPF (Verilog extended Berkeley Packet Filter) firewall for FPGA-based IoT devices. This VeBPF firewall accepts standard eBPF bytecode as firewall rules; these rules are run by VeBPF CPU cores. Any number of VeBPF cores can be generated by specifying the N_{VeBPF} parameter.

II. Multi-Core Multi-Rule VeBPF Firewall

In order to run eBPF bytecode on the VeBPF firewall, we have developed a VeBPF CPU core (Fig. 1), which is eBPF ISA compliant. A few details are omitted, but these are purely related to the software OS (e.g., the *call* instruction which we modified to integrate custom hardware accelerators).

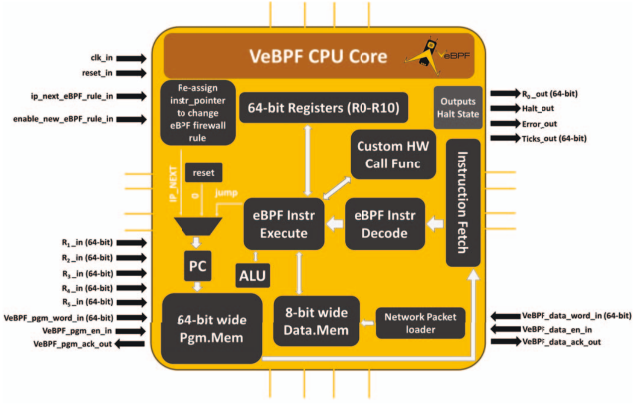

Fig. 1: VeBPF CPU core computer microarchitecture.

The overall architecture of the multi-core multi-rule VeBPF firewall for FPGA-based IoT devices is show in Fig. 2. The various subsystems that make up the VeBPF firewall, along with additional subsystems, are a part of our larger hardware OS project: highly flexible, loosely-coupled subsystems are being developed that use native tool-chains and drivers. These include eBPF (for the VeBPF firewall) and VirtIO [1], [2].

The novel contributions of our work are the designs of the various finite state machines (FSMs) for implementing any number of eBPF firewall rules, plus generation and integration of any number of VeBPF CPU cores as specified with the N_{VeBPF} parameter. The only limitation on the number of VeBPF CPU cores or the number of eBPF firewall rules is the resources available on the FPGA-based IoT device. The VeBPF firewall FSMs are designed so that more VeBPF cores leads to faster processing of the eBPF firewall rules on the network packets.

We evaluated the multi-core multi-rule VeBPF firewall on a Xilinx Arty A7-100T board at 100 Mbps network throughput. The VeBPF firewall was able to filter network packets at line rate as compared to a RISC-V softcore which was not able to keep up with the throughput and latency.

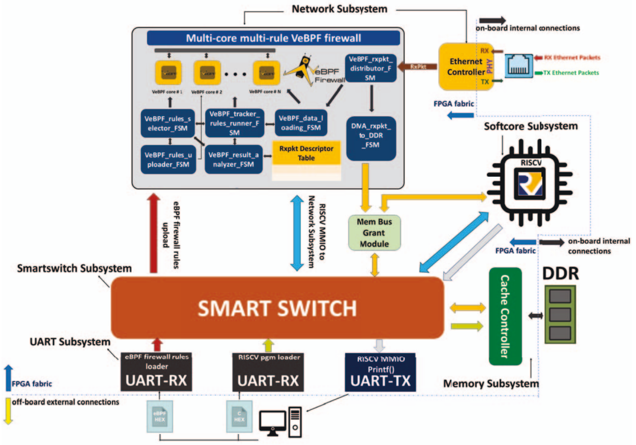

Fig. 2: Multi-rule Multi-core VeBPF Firewall architecture.

Acknowledgments

This work was supported, in part, by the NSF through awards CCF-1919130 and CCF 2151021; and by Red Hat through awards 2023-01-RH13 and 2024-01-RH08.

References

[1] S. Bandara, A. Sanaullah, Z. Tahir, U. Drepper, and M. Herbordt, "Enabling virtio driver support on fpgas," in *2022 IEEE/ACM International Workshop on Heterogeneous High-performance Reconfigurable Computing (H2RC)*, 2022, pp. 1–8.

[2] S. Bandara, A. Sanaullah, Z. Tahir, U. Drepper, and M. Herbordt, "Performance Evaluation of VirtIO Device Drivers for Host-FPGA PCIe Communication," in *2024 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, 2024.

979-8-3503-6460-6/24/$31.00 ©2024 IEEE
DOI 10.1109/IPDPSW63119.2024.00053