Transparent malicious traffic detection using a BlueField DPU

Authors:
Jelle Ermerins (jermerins@os3.nl)
Ward Bakker (wbakker@os3.nl)

Supervisor:
Cedric Both (cedric@datadigest.nl)
Introduction

- Processing large amounts of traffic can be heavy on the CPU
- Network Interface Cards (NICs) can process traffic more efficiently
- Limited performance on certain operations
- Cryptographic, memory, regular expressions operations
- Offloading to a Data Process Unit (DPU)

- Detect / Block Malicious traffic using an IDS/IPS
- Can be done on a separate machine
  - ... or on a DPU, transparently
- Cost efficient, programmable
The NVIDIA Bluefield-1 DPU

- SmartNIC containing a DPU
- Offloading certain operations, in a transparent way
- Contains an ARM based System-on-Chip
- Might be useful for running IDS/IPS software on the SoC itself
Related Work

- Liu et al. [1] stress the Bluefield SmartNIC using stress-ng
  - Show that the Bluefield is good at certain operations when offloaded, like memory or cryptographic operations
  - Avoid kernel network stack: use userspace or hardware-accelerated solutions

- Zhang et al. [2] researched optimizing Snort using the DPDK
  - Using DPDK for Snort resulted in better performance

- We look at what optimizations are possible, for IDS specifically
- And what is possible on the Bluefield DPU and what are the limitations
  - When processing large amounts of (malicious) traffic
Research Questions

*What are the limitations of the NVIDIA Bluefield SmartNIC regarding the detection of large amounts of malicious traffic?*

- What are the possibilities regarding the optimization of IDS software within the Bluefield DPU?
What is possible regarding IDS/IPS optimization?

NVIDIA DOCA SDK [3]
- Software Development Kit for applications on the Bluefield DPU.
- Deep Packet Inspection (DPI) [4]
  - Identify and block malicious traffic

DPDK: Data Plane Development Kit [5]
- Libraries to accelerate packet processing
- Offload packet processing from the kernel to processes in userspace
- Some projects using Suricata and Snort IDS with DPDK [6][7]
- OvS DPDK [8]
What is possible regarding IDS/IPS optimization?

XDP: Express Data Path

- Adds early hook in the RX path of the kernel
- Requires kernel module, which means compile your own kernel
- Have support within the network card driver
- Enable XDP in Suricata IDS [9]
Modes of Operation

Separate Mode

- Host and DPU act as separate entities
- The host just uses the Bluefield as a NIC

Embedded (SmartNIC) Mode

- All traffic to and from the host goes through the DPU
- In a transparent way
- In this mode we can install software on the DPU (like an IDS)
Setup

- **Send traffic using Cisco TRex**\(^{[10]}\)
  - UDP and TCP with random data
  - Realistic Malicious Traffic
  - 1, 10, 25, 50, 100Gbps

- **TRex**
  - Uses DPDK and Scapy
  - Is able to generate 200Gbps of UDP & TCP Traffic

- **Realistic Malicious Traffic**
  - Generated pcap based on Suricata ruleset \([11][12]\]
  - Replay pcap
  - Change delay between packets to vary throughput
Setup

- Send traffic using Cisco TRex
- Run Suricata IDS/IPS on Bluefield ARM
  - Emerging Threats OPEN Ruleset
  - Added custom rules that alert/drop all TCP/UDP packets
- IDS Mode
  - Alongside OvS
  - Only alerts
- IPS Mode
  - Without OvS
  - Alert, or drop packets
Setup

- Send traffic using Cisco TRex
  - UDP, TCP
  - Realistic Malicious Traffic
  - 1, 10, 25, 50, 100Gbps
- Run Suricata IDS/IPS on Bluefield ARM
- Measure incoming bps on ARM and Host
Results - (Without) Suricata in IDS Mode
Generated TCP & UDP Traffic
Results - (Without) Suricata in IDS Mode
Generated TCP & UDP Traffic
Results - Suricata in IPS Mode - Alert Generated TCP & UDP Traffic
Results - Suricata in IPS Mode - Alert
Malicious Traffic based on Suricata Ruleset

1Gbps Malicious Traffic - Suricata in IPS Mode (Alert Only)

- Received on Bluefield
- Received on Host

Traffic Received (Mbps)

Time (s)
Results - Suricata in IPS Mode - Drop

- Almost all packets dropped on Bluefield, no incoming packets on Host
  - As expected
- Short ‘leak’ periods of couple packets
Discussion

● The interfaces are capable of 100Gbps
● Processing 100Gbps can’t be done using the DPU*
  ○ At 100% CPU load, max throughput ~250Mbps
  ○ *As standalone device, 100Gbps is possible
  ○ *The applications like OvS, Suricata limit the performance
● Missing Regular Expression acceleration
● High(er) packets loss each time the throughput increases
Limitations

- Unfortunately, DOCA SDK not available on Bluefield-1
- DPDK with Suricata work in progress
- OvS DPDK exists but couldn’t get it working properly on the Bluefield
- Missing kernel XDP module
Conclusion

What are the limitations of the NVIDIA Bluefield SmartNIC regarding the detection of large amounts of malicious traffic?

- With the Bluefield we can send & receive 100Gbps of traffic
- Running Suricata & OvS has impact on the performance
  - It cannot handle the detection / processing large amounts of malicious traffic
- Optimizations that could improve performance are hard to implement on the Bluefield-1
Future work

- Experiment with the Bluefield 2 DPU, that supports DOCA
  - Compare performance of DOCA Deep Packet Inspection as an IDS to Suricata or Snort
- Research other optimizations of IDS software
  - DPDK, XDP & eBPF
- Optimizations regarding OvS on the Bluefield
Questions?
References


    https://blog.mellanox.com/2020/04/xdp-acceleration-over-mellanoxs-connectx-nics/


[12] https://github.com/felixe/idsEventGenerator
Backup slides
Cisco Traffic Generator (Trex)

- Open source realistic traffic generator traffic generator
  - Uses:
    - Data Plane Development Kit (DPDK)
    - Scapy
    - Python
  - Supports OSI layer 3 to layer 7
  - Supports modes:
    - Stateful
    - Stateless
- Benchmark / Stresstest