Hardware acceleration of IDS for high-speed networks

Lukáš Kekely (kekely@cesnet.cz)
17th July 2017, 43rd NMRG meeting
Liberouter group

- guarding the perimeter of CESNET
Toolset

Netopeer
NETCONF Remote Configuration

Flow Probe
Flow Probe
Flow Probe
Flow Probe
Flow Information Export
Data Acquisition

Flow Collector
Data and Statistics Storage

Applications
Visualisation
Anomaly Detection
QoS Measurement

Network Line(s) with TAP(s)
Presentation scope
Monitoring probe

- **Standard approach:**
  - operation as standard NIC (capturing packets)
  - software processing of the whole traffic

- **Accelerated approach:**
  - accelerated traffic preprocessing in card
  - SW performs advanced/specific processing
  - our unique concept of: 
    
    Software Defined Monitoring
SDM concept

Firmware

- Rules
  - Flow Cache
  - Actions
  - Rule Lookup
  - UHs
  - Parser

Software

- SDM Controller
- Preprocessing Requests
- DMA Buffers
- App 1
- App N
- Flow Exporter

Packets

IPFIX
SDM results

- Monitoring tasks can be accelerated
  - INFOCOM paper, IEEE ToC article

- Can SDM be used to accelerate IDS?
IDS assumptions

1. performance of software IDS is limited
   ○ insufficient for current multi Gbps networks

2. default discarding method is blind
   ○ input buffer overflow if IDS is not fast enough

3. informed drops enable better results
   ○ IDS packet processing rate is the same
   ○ more interesting data are processed

4. the most relevant are initial packets

5. majority of traffic belongs to few flows
   ○ only drop trailing packets of a few heavy flows
IDS over SDM

Firmware

Rules

Actions

Rule Lookup

UHs

Parser

Packets

Software

SDM Controller

Drop Requests

IDS th1

DAT a B us

DMA Buffers

IDS thN

Reporting
Test setup

- Tested IDS:
  - Suricata
  - Snort
Test server

- Supermicro X9DRG-QF server
- 2x Intel Xeon E5-2650 (8x 2.6GHz)
- 64GB DDR3 RAM
- acceleration COMBO card:
  - 10x 10 Gbps Ethernet ports
  - line rate 100 Gbps capture
  - Xilinx Virtex-7 FPGA
  - SDM firmware
Snort @ libpcap

The graph shows the comparison of buffer overflow and detected events between Snort without SDM and with SDM at different speeds up to 2000 Mbps. The green line represents the scenario without SDM, while the red line indicates the scenario with SDM.

- **Buffer overflow [%]**: The green line (without SDM) shows a steady increase from 0 to approximately 80% as speed increases. The red line (with SDM) remains at a low level, staying below 20%, indicating a significant reduction in buffer overflow with SDM.

- **Detected events**: The green line (without SDM) significantly decreases as speed increases, dropping from above 200 events to below 50 events. The red line (with SDM) also decreases but remains higher than the green line, indicating fewer detected events with SDM compared to without SDM.

This graph highlights the effectiveness of SDM in managing buffer overflow and reducing detected events at high speeds.
Suricata @ libpcap
Suricata @ SZE2

---

**Graph 1:**
- **Y-axis:** Buffer overflow [%]
- **X-axis:** Speed [Mbps]
- Lines:
  - Green: without SDM
  - Blue: with SDM-SOFT
  - Red: with SDM

**Graph 2:**
- **Y-axis:** Detected events
- **X-axis:** Speed [Mbps]
- Lines:
  - Green: without SDM
  - Blue: with SDM-SOFT
  - Red: with SDM
Suricata (small) @ SZE2

The graph shows the buffer overflow and detected events percentage with different speeds and configurations:

- **Buffer overflow [%]**
  - Green line: without SDM
  - Blue line: with SDM-SOFT
  - Red line: with SDM

- **Detected events**
  - Green line: without SDM
  - Blue line: with SDM-SOFT
  - Red line: with SDM

The x-axis represents speed in Mbps, ranging from 10000 to 25000 Mbps.
Summary

- IDS can be accelerated by SDM
  - significantly reduced packet loss
  - higher achievable processing throughput
  - better detection accuracy at faster lines

- SDM is applicable in yet another area
  - designed primarily for monitoring
  - can accelerate security applications as well

- INFOCOM paper in preparation
Thank you for your attention!

More info:
- https://www.liberouter.org/
- kekely@cesnet.cz