Hardware Acceleration of Intrusion Detection Systems for High-Speed Networks

Jan Kučera
CESNET a.l.e.
Prague, Czech Republic
jan.kucera@cesnet.cz

Lukáš Kekely
CESNET a.l.e.
Prague, Czech Republic
kekely@cesnet.cz

Viktor Puš
Netcope Technologies
Brno, Czech Republic
pus@netcope.com

Adam Piecek
FIT BUT
Brno, Czech Republic
xpiece00@stud.fit.vutbr.cz

Jan Kořenek
IT4Innovations Centre of Excellence, FIT BUT
Brno, Czech Republic
korenek@fit.vutbr.cz

ABSTRACT

Intrusion Detection Systems (IDS) are among popular technologies for securing computer networks. However, their high computational complexity makes it hard to meet performance goals of modern high-speed networks. This paper aims at an acceleration of IDS by informed packet discarding. Focusing the limited computational resources available to IDS towards only the most relevant parts of incoming traffic and offloading (bypassing) the rest. We show that this controlled (informed) discarding of well-defined traffic portions helps IDS to achieve better results and compare software and FPGA accelerated discarding implementations.

CCS CONCEPTS

• **Security and privacy → Network security**; • **Hardware → Hardware accelerators**;

KEYWORDS

Suricata IDS, high-speed networks, hardware acceleration

ACM Reference Format:
Jan Kučera, Lukáš Kekely, Viktor Puš, Adam Piecek, and Jan Kořenek. 2018. Hardware Acceleration of Intrusion Detection Systems for High-Speed Networks. In *ANCS '18: Symposium on Architectures for Networking and Communications Systems, July 23–24, 2018, Ithaca, NY, USA.* ACM, New York, NY, USA, Article 4, 3 pages. https://doi.org/10.1145/3230718.3232114

ANCS '18, July 23–24, 2018, Ithaca, NY, USA
© 2018 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-5902-3/18/07.
https://doi.org/10.1145/3230718.3232114

1 INTRODUCTION

To aid the performance of a general software-based IDS without hindering its flexibility, we propose a controlled reduction of the traffic amounts that it must process. Based on basic characteristics some packets are deemed interesting and processed, while others are discarded. The selection is done in such a way that the negative impacts on IDS detection abilities are minimal. The proposed IDS acceleration concept builds on the assumptions that the most relevant information regarding security is present in several packets at the beginning of each network connection (flow), and that discarding the majority of subsequent packets do not significantly reduce the IDS quality of threat detection.

2 SYSTEM DESIGN

Since we assume that the most relevant information regarding security is present in several packets at the beginning of a network connection, we design our concept to drop all packets that follow the first N packets of each network flow. The value of threshold N is arbitrarily altered depending on momentary network situation. Of course, because of this design choice, the system does not detect attacks which arise after the first N packets of the flow, but our preliminary analysis has shown that the number of such attacks is very small (less than 10 % even for $N = 30$).

To perform the described decision, a system implementing the proposed input concept must maintain at least very basic flow statistics. This requires implementation of two main additional modules: *packet header parser* to extract flow identification and *network flow cache* to store flow lengths. The packet is dropped if the counter for appropriate flow exceeds configured threshold N otherwise, the packet is forwarded to IDS for normal processing. This form of operation is general and independent on the particular features of used IDS.

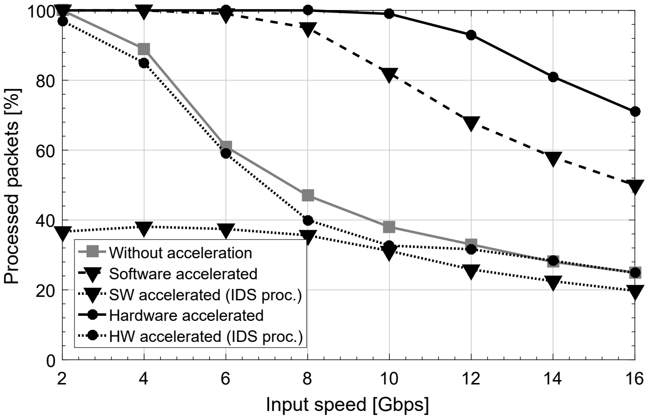

Figure 1: Packets processed at different speeds.

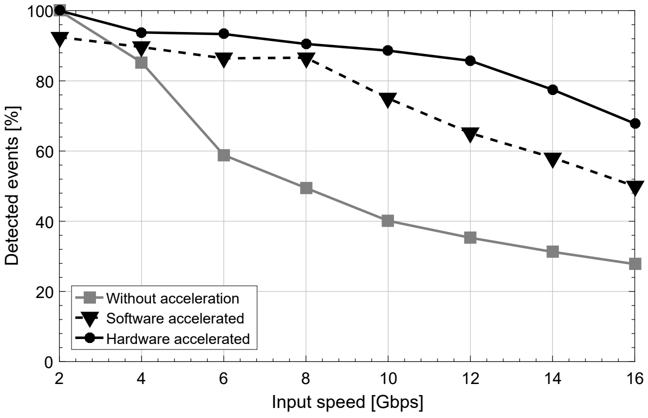

Figure 2: Security events detected at different speeds.

Utilization of the proposed input system inevitably requires some additional processing from the CPU, adding to its total load. Therefore, we employ hardware accelerator that drops unwanted packets before they even reach the CPU. Both the packet parser and the network flow cache must be present in the utilized hardware accelerator so that the decision whether to drop or pass packets can be offloaded and made directly by the accelerator. To implement the hardware accelerated version of our concept, we utilize a subset of the Software Defined Monitoring (SDM) functionality [1], which is primarily designed for network monitoring, but here we show that it is also usable in IDS acceleration.

3 EXPERIMENTAL RESULTS

The proposed acceleration concept is evaluated using Suricata IDS [2] with all of the 13 642 detection rules from the EmergingThreats database [3]. It is running on a commodity SuperMicro server with 8 core Intel Xeon E5-2670 CPU and 64 GB of RAM. We use unsampled packet data acquired from our nation-wide network. The captured PCAP file contains 285 833 947 packets of 8 642 744 flows in over 200 GB of data. The traffic is replayed on its original capture speed of 2 Gbps and packet replication (with modification of IPs) is used to achieve higher throughputs. Three IDS deployment scenarios are evaluated and compared: without acceleration, software accelerated, and hardware accelerated.

Figure 1 shows packet drop rates for each of the tested scenarios. For non-accelerated version (grey solid line, squares), Suricata starts uncontrolled packet drops at an input rate above 2 Gbps. For accelerated versions, most of the packets never even reach the IDS processing (black dotted lines). This significantly helps in reducing uncontrolled packet drops at the system input (dashed and solid black lines). The limited CPU performance forces even the accelerated system to eventually drop some of the packets uncontrollably, but this occurs at much higher speeds. Figure 2 plots the percentage of detected events in the described cases (100 % is given by offline analysis of the PCAP). The percentage of all events detected lowers rapidly with the uncontrolled packet drops. However, the presence of *controlled* discarding in accelerated versions (black circles and triangles), causes only a moderate decline in detection quality. In hardware accelerated scenario (black solid line, circles), the detection rate drops under 80 % only at speeds higher than 12 Gbps, while without acceleration (grey solid line, squares) this drop occurs right after 4 Gbps mark (3× sooner). From a different perspective, the detection quality of Suricata IDS is enhanced up to 2 or 3× by the proposed hardware acceleration at higher input speeds.

4 CONCLUSION

We have designed a general concept of IDS acceleration based on a controlled (informed) reduction of incoming traffic. Experimental results using Suricata and data from a real high-speed network show that the controlled discarding is better than default buffer overflow. The IDS is able to **process up to 3× higher input speeds**, while high detection quality is maintained. From a different point of view, our acceleration enables an overloaded IDS to **detect around 3× more events** compared to the case without acceleration.

Acknowledgment. This research is supported by the project Reg. No. CZ.02.1.01/0.0/0.0/16_013/0001797 by the MEYS of the Czech Republic; the IT4Innovations excellence in science project IT4I XS – LQ1602; and by the Ministry of the Interior of the Czech Republic project VI20172020064.

REFERENCES

[1] L. Kekely, J. Kučera, V. Puš, J. Kořenek, and A. V. Vasilakos. 2016. Software Defined Monitoring of Application Protocols. *IEEE Transactions on Computers* 65, 2 (Feb 2016), 615–626. ISSN: 0018-9340.

[2] Matt Jonkman et al. Suricata. (2017). http://suricata-ids.org

[3] proofpoint. Emerging Threats. (2017). https://rules.emergingthreats.net