Balancing between Power Efficiency and High Performance on Software-based Intrusion Detection System

Muhammad Jamshed, Jaehyun Nam, Byungkwon Choi, Dongsu Han, and KyoungSoo Park
Department of Electrical Engineering
Korea Advanced Institute of Science and Technology (KAIST)

Abstract

Recent research on intrusion detection systems (IDSes) has mainly focused on improving the traffic analyzing rate to meet the increasing bandwidth requirements [4], [5]. This has prompted the rise of hybrid usage of CPUs and GPUs well as FPGA/ASIC-based IDS systems that scale well to tens of Gbps of the ingress traffic rate [2], [3], [6]. One noticeable concern with these systems, however, is that they typically become a power hog that consumes several hundreds (up to a thousand) of watts of processing power. In recent years, low-powered programmable many-core processors (MCPs) have actively reduced the power usage despite with tens of processors. Although IDSes running on MCP hardware show promising results, they fail to scale at ingress rates of 10+ Gbps due to (i) high memory access contention and (ii) increased branched instruction prediction misses.

In this work, we seek the right balance between power efficiency and high performance on signature-based IDS on a Tilera board [1]. In normal situations, our system analyzes entire ingress traffic in a power-efficient way, solely using the co-processor. However, when the system is under stress (opportunistic offloading mode), the IDS starts delegating subtasks to the host system. We have devised the offloading mode in two flavors. (i) In a *flow-centric offloading* mode, only the packets from new connections bypass the MCP and are directly forwarded to the host system for comprehensive analysis. (ii) In a *functional offloading mode*, the entire ingress traffic is first processed by the MCP; and only suspect flows (that pass the first stage of multi-attack string pattern matching phase) are subsequently offloaded to the host system for further analysis. We compare the effectiveness of these approaches and aim to achieve a multi-10 Gbps analyzing rate while consuming only a few tens to hundreds of watts.

References

[1] Tilera: Tile-gx processor family. http://www.tilera.com/products/processors/TILE-Gx_Family.

[2] C. Clark, W. Lee, D. Schimmel, D. Contis, M. Kone, and A. Thomas. A hardware platform for network intrusion detection and prevention. In *In Proceedings of the 3rd Workshop on Network Processors and Applications (NP3), February 2004. 178.*

[3] M. A. Jamshed, J. Lee, S. Moon, I. Yun, D. Kim, S. Lee, Y. Yi, and K. Park. Kargus: A highly-scalable software-based intrusion detection system. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 317–328, New York, NY, USA, 2012. ACM.

[4] R. Smith, C. Estan, and S. Jha. Xfa: Faster signature matching with extended automata. In *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, SP '08, pages 187–201, Washington, DC, USA, 2008. IEEE Computer Society.

[5] G. Vasiliadis, S. Antonatos, M. Polychronakis, E. P. Markatos, and S. Ioannidis. Gnort: High performance network intrusion detection using graphics processors. In *Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection*, RAID '08, pages 116–134, Berlin, Heidelberg, 2008. Springer-Verlag.

[6] G. Vasiliadis, M. Polychronakis, and S. Ioannidis. Midea: A multi-parallel intrusion detection architecture. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 297–308, New York, NY, USA, 2011. ACM.