Multicore CPUs for Parallelizing Network Intrusion Prevention

As technology progresses, human beings become more and more dependent on the machines in their everyday life. The current age presents us with a level of interconnect that far surpasses anything else in history. Digital communication is, thus, of paramount importance for individuals and businesses alike. As the amount of data going back and forth increases, the process of protecting it requires more and more resources.

The current thesis is focused on improving the process of network intrusion and prevention through the use of parallelism. On modern hardware architectures, parallelism is often associated with multicore CPUs and GPUs. The research presented here looks at the available parallel technologies and explores the benefits they can bring to different areas of network security. The thesis approaches different themes by presenting some theoretical notions and concepts, along with the current state of the art. New areas of improvement are suggested, and supported by experiments involving parallel technologies.

The thesis begins by investigating performance bottlenecks of existing security solutions. The investigation is performed in the context of modern operating systems and hardware architectures. Open source intrusion detection and prevention systems are presented in detail, with the elements that drive security processes in mind: traffic filtering, file scans, malware detection, etc. The problem of security is analyzed from the point of view of the individual users, as well as an enterprise. The main performance vectors are identified as detection accuracy, speed and power consumption. The following experiments will be set to improve these items.

Pattern matching is identified as an important aspect of network security (used in signature and rule matching). The research around pattern matching is focused around its parallelization using APIs such as OpenCL on a wide range of devices. The comparative performance between the OpenCL-GPU implementation and multicore-CPU is discussed in terms of parallel speedup and power consumption. The thesis presents hybrid experiments that opportunistically use the computing power of the CPU and GPU in order to achieve the best performance. The discussion targets distributed security systems deployed inside the network and host-based solutions like antiviruses.

Instruction-level parallelism is presented as an important feature in accelerating encryption and hashing processes inside a NIDPS. Instruction-level parallelism is present in the form of complex instruction scheduling algorithms inside the CPU core or SIMD extensions of the instruction set (SSE, AVX, NEON). An experiment comparing the impact of parallelism on encryption and decryption using stream ciphers is presented in the context of network security.

The subject of machine learning is presented as an upcoming trend in network security. Machine learning stages such as training and deployment benefit from parallelization. The thesis discusses data acquisition techniques and tracing in the context of parallel network intrusion detection. The topic of visualization and human reaction to security incidents is also discussed.

The thesis concludes with a summary and highlight of the most important personal contributions and issues some considerations regarding future research directions.