Next-Generation Virtual Memory Abstractions and Mechanisms to Ensure their Security.

Guilherme Mota Cavalcanti A Cox
Dept. of Computer Science

4/28/2017 at 03:00 pm
CoRE A (301)

Abstract

The emergence of big-data workloads in the analytics, business, and scientific computing domains, allied with the advent of new compute technologies (e.g., GPUs, FPGAs, neural network accelerators) and memories (e.g., persistent byte-addressable memory, die-stacking memory, etc.) warrants a rethink of fundamental systems abstractions. A central abstraction is that of virtual memory. Virtual memory allows us to program systems with a myriad of compute resources in a tractable manner, while harnessing their benefits. However, the virtual memory abstractions we use today have remained unchanged from the time of mainframes made up of discrete transistors. Naturally, these traditional VM abstractions are antiquated and woefully inadequate in today's vastly different computing landscape.

My talk presents hardware and operating system support to realize a modern virtual memory abstraction for modern systems. A central tenet of my work is to design hardware that unobtrusively inspects OS/program activity (without changing them) to realize efficiency, better performance, and energy-efficiency. Further, I will discuss low-overhead mechanisms to ensure that changes to the virtual memory stack – a systems layer often prone to security exploits – remain secure in addition to being efficient.

Examination Committee: Prof. Abhishek Bhattacharjee (Chair), Prof. Vinod Ganapathy, Prof. Ulrich Kremer, Prof. Ahmed Elgammal.