Project: Architectural Support for Security and Trusted Computing in Multi-Core Processors

Investigators: Nael Abu-Ghazaleh and Dmitry Ponomarev

Summary: Modern multicore and manycore architectures have a number of new security threats. For example, shared microarchitecture components such as caches, core inter-connection networks, and memory controllers can be exploited for side-channel attacks or denial of service attacks. The new workloads that exploit explicit parallelism will also likely lead to additional new threats. New forms of active viruses and trojans that reside on some cores and attempt to attack other applications are likely to arise. It is critical to anticipate such new forms of threats and design multi-core and manycore systems in a manner that facilitates defeating them. If security is not treated as a first order design principle, these systems will be highly vulnerable to attacks, leading to enormous losses in money and productivity and a substantial effort to retrofit security in after the fact.

The overall theme of this project is to identify and analyze security threats that can arise in a multicore and manycore environment and develop algorithms and techniques to address these threats in a complexity-effective manner and without sacrificing performance. Specific interest is on the techniques and solution patterns that can be reused to help with different threats. These include the use of additional cores and thread contexts to provide security without significant performance losses, and the development of techniques for virtual and physical isolation of shared resources to defend against side-channel attacks and denial-of-service attacks. For example, a spare processing core or a spare hardware thread context can be used to efficiently support dynamic information flow tracking or memory bounds checking in hardware by offloading all security monitoring logic to a separate core and keeping the changes to the main core to the minimum.

In addition, the project explores approaches for trading-off performance and security and also considers security vulnerabilities of new memory technologies. Another direction pursued in this project is the design and evaluation of Trusted Platform Modules (TPM) suitable for the use in multicore systems from both correctness (security) and performance standpoints.