Dynamic Spatially Isolated Secure Zones for NoC-based Many-core Accelerators

Maria Méndez Real[1], Vincent Migliore[1], Vianney Lapotre[1], Guy Gogniat[1],
Philipp Wehner[2], and Diana Göhringer[2]

[1]Univ. Bretagne-Sud, UMR 6285, Lab-STICC,, F-56100 Lorient, France, maria.mendez@univ-ubs.fr
[2]Ruhr-University Bochum, Germany, {philipp.wehner, diana.goehringer}@rub.de

Abstract

Many-core architectures are becoming a major execution platform in order to face the increasing number of applications executed in parallel. While many-core accelerator architectures offer users with massive parallelism and high performance, it also introduces some key challenges in terms of security. Indeed, in order to leverage performance, a great number of applications running in parallel may share resources. A malicious application may compromise other applications sharing resources with or the whole system by directly accessing, deducing or retrieving sensitive data. A defense-in-depth approach relying on hardware and software mechanisms is thus mandatory to increase the level of protection. This work focuses on a many-core accelerator architecture extended with mechanisms allowing the logical and spatial isolation of sensitive applications through the dynamic creation of secure zones. Each sensitive application is executed within a secure zone avoiding any resource sharing with other potentially malicious applications. In this way, denial of services and confidentiality and integrity attacks are prevented. In order to achieve this goal, a set of services guarantying the dynamic creation and handling of spatially isolated secure zones in a many-core accelerator architecture are proposed. These services are integrated into a software controller on a many-core accelerator architecture and evaluated through virtual prototyping in terms of security level and induced performance overhead.