NOC-BASED DYNAMIC SECURITY IMPLEMENTATION FOR MULTI-APPLICATION SOC

Martha Johanna Sepulveda, Guy Gogniat, Wang Jiang,
Marius Strum, Ricardo Pires and Cesar Pedraza

SoC designers have to face tight development times as well as the rapid evolution of current applications. To be cost effective, SoCs are often programmable and integrate several different applications on the same chip (i.e. cell-phone, personal digital assistant). Although sharing many of the hardware components on the SoC, different applications executed on the same die may present very different requirements and design constraints. Such type of system is called multi-application. MPSoCs (Multi Processor System-on-Chip) have been proposed as a promising architecture choice to overcome the new challenging application requirements. The MPSoC platform allows the execution of several applications in the same structure. Such flexibility also represents a system vulnerability. Each application supported by the MPSoC is characterized by different sets of security rules, called security policy. The set of applications can be mapped dynamically at the MPSoC. Therefore, there is not a single and static security requirement, but a set of ever changing security policies that must be satisfied. The challenge is to provide MPSoC security that allows a trustworthy system that meets all the security requirements of such applications. MPSoC can be attacked via hardware/software.

Software attacks are responsible for 80% of the security incidents. All software attacks start with an abnormal communication. In this talk we address protection of the MPSoC against the software attacks by the implementation of a hierarchical security NoC-based architecture. It integrates agile and dynamic security firewalls into the NoC in order to detect attacks based on different security rules. In order to support the MPSoC high communication requirements the Network-on-Chip (NoC) is employed. A NoC is an integrated network that uses routers to allow the communication among the computation structure components.

The NoC may contribute to the overall security of the system, providing the ideal mean for monitoring systems behavior and detecting specific attacks. The communication structure is becoming the heart of the MPSoC. It has a significant impact on the overall MPSoC performance. To make feasible the MPSoC protection by NoCs, the security must be customized, in order to provide a better trade-off between the system performance and the security. We propose the implementation of QoSS (Quality of security service) to overcome present SoC vulnerabilities. QoSS is a novel concept for data protection that introduces security as a dimension of QoS (Quality-of-Service). QoSS uses a Network-on-Chip (NoC) to provide predictable security levels of the system by adding functionality to the routers of the network and consequently changing some local configuration parameters or modifying the network interfaces.

Our hierarchical approach distributes the security policy management by partitioning the NoC topology into different security zones (low NoC), ruled by a local security policy. Different security zones are connected through a global interconnect (high NoC), ruled by a global security policy. Our approach provides an effective way to handle security policy changes and improves the overall system performance. Each zone integrates a set of mechanisms capable of being configured according to the QoSS needs of each application. The different levels of security of each security zone arise from the configuration of the parameters of the NoC security mechanisms. Two techniques are employed in order to achieve an efficient configuration: 1- the security mechanisms are implemented hierarchically therefore avoiding the NoC interruption; and 2- QoS (Quality-of-service) mechanisms are employed to provide predictable penalties while the network interfaces are modified. The experiments were performed using a SystemC-TLM timed simulation framework. It automatically carries out performance evaluations for a wide variety of MPSoC scenarios. We show that our architecture can perform a fast detection of a wide range of attacks and a fast configuration of the different security policies for several MPSoC applications. We also show that the penalties due to the integration of the dynamic NoC-based security architecture are limited to a fraction of time and space of the system.