Validation of SoCs Security Architecture: Challenges, Threats, and Methods

Dr.-Ing Mehran Goli, University of Bremen/DFKI Bremen, Germany

The increasing deployment of computing devices in a large number of highly personalized activities and critical aspects of our lives (e.g., medical devices, automobiles, flight control, and banking systems) has raised their requirements on security significantly. Modern computing systems are typically implemented as system-on-chip (SoC) designs, namely a single integrated circuit containing the system functionality. An SoC design involves the composition of a large number of Intellectual Properties (IPs) such as memories, processing units, I/O interfaces, and other various hardware accelerators (e.g., hardware encryption units). These IP blocks are integrated through a number of on-chip interconnects (buses) to implement the system functionality. Since data (including secure assets) in such a system is transferred via the shared interconnects across different IPs, access control or information flow requirements are defined by a collection of security policies. The policies specify the conditions under which a secret asset can be accessed at any point in the system execution. Thus, an SoC needs a security architecture to ensure that the system enforces and manages these policies e.g., a mechanism of authentication or managing access to shared resources.

Over the past few years, Information Flow Tracking (IFT) has been shown as a powerful technique to help mitigate security vulnerabilities that violate certain information flow policies and noninterference properties. IFT works by monitoring how information propagates through a system to see if secret information is leaking to an untrusted subsystem or to ensure that the integrity of a critical subsystem is not violated.

Since the cost of fixing any security flaws increases with the stage of development, the validation process should be performed as early as possible. For the early design entry, Virtual Prototype (VP) is being increasingly adopted by the semiconductor industry. A VP is an abstract and executable software model that is typically implemented using SystemC and its Transaction Level Modeling (TLM) framework at the Electronic System Level (ESL). In comparison to the Register Transfer Level (RTL) designs, VPs provide designers with orders of magnitude faster simulation speed. By this means, a system can be implemented quickly and used as a reference model for lower levels of abstraction. Hence, we believe VP-based security validation could be one promising direction to fix the security vulnerabilities in the SoCs before they are refined and to avoid costly design loops occur. We discuss the security threat models at the ESL, the challenges to detect security flaws related to non-interference property and introduce validation approaches to block such behavior.