NoC cover and side channels are real: And now?

Johanna Sepulveda[1], Cezar Reindbrecht[2], Lilian Bossuet[2], Guy Gogniat[3], Georg Sigl[1]

[1]Institute for Security in Information Technology, Technical University of Munich, Germany
[2]Hubert Curien Laboratory, UMR 5516 CNRS, University of Lyon at Saint-Etienne, France
[3]Lab-STICC, South Brittany University, France

johanna.sepulveda@tum.de

Multi-Processors Systems-on-Chip (MPSoC) are vulnerable and can be attacked. One of the major MPSoC dangerous threats appears from the resource sharing, when malicious and sensitive processes are executed together. Network-on-Chip (NoC), the shared MPSoC communication structure, presents several cover and side channels which can be exploited to reveal sensitive communications. Data-dependent timing characteristics of some security functions can be exploited through communication collision attacks. Access pattern and volume of the communications may reveal the sensitive information.

This talk is divided into three parts that present the aspects for the NoC-based MPSoC timing attacks. The first part presents the threat model and the cover and side channels in the NoC. The second part shows two practical timing attacks on MPSoCs based on simple communication collision and the enhanced Prime+Probe technique. Finally, the third part presents some of the protection techniques able to be implemented in the NoC routers, links and Network interfaces. We show the security efficacy, performance and cost of our protection techniques.