Rising demands for increased performance, lower energy consumption, connectivity and programming flexibility are nowadays driving the platforms, so-called Multi-Processor Systems-on-Chips (MPSoCs). These platforms are composed of several processing elements, custom IP cores, and memories, all of which are in general interconnected by a Network-on-Chip (NoC). As attractive as these characteristics are, they introduce several security concerns, specially when applications with different trust and protection levels share resources. When a malicious software acquires access to an IP, it opens a door to external surveillance of the cache-memory, processing units and the NoC communication structure. The cache memory was already exploited by several authors in ASICs and Systems-on-Chips through Side-Channel Attacks (SCAs). In this work, we expand this concept, exploring the timing attacks on caches in the MPSoC scenario. We implement two well established attacks in the literature on a real hardware platform, the MPSoC Glass. Furthermore, we present the NoC as a novel vulnerability to increase attack efficiency, resulting in the Earthquake Attack. Results show that the attacks from literature can
succeed inside the MPSoC, and obtain better results. Additionally, Earthquake improves the base attack by using the NoC timing attack, reducing the remaining attack complexity from 236:9 to 232 with 216:6 encryptions instead of 227:97.

Stichworte:

Dewey Dezimalklassifikation (Liste):
620 Ingenieurwissenschaften

Kongress- / Buchtitel:
Microprocessors and Microsystems: Embedded Hardware Design (MICPRO)

Jahr:
2019

Serien-ISSN:
01419331

WWW:
https://www.evise.com

Occurences:
- Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2019

Entries: