Towards Trace-driven Cache Attacks on Systems-on-Chips – Exploiting Bus Communication

The growing complexity of Systems-on-Chips (SoCs) increases the risk of software attacks during runtime. A critical threat to system security are so-called side-channel attacks based on the processor cache and its usage during the execution of cryptographic algorithms. Recent publications have analyzed cache attacks on mobile devices and network-on-chip platforms. In this work, we investigate cache attacks on bus-like tile-based Multi-Processor Systems-on-Chips (MPSoCs). This work presents two contributions. First, we demonstrate a trace-driven cache attack on AES-128 based on the exploitation of bus communication. Second, we integrate two countermeasures (Shuffling and Minitable) and evaluate their impact on the trace-based cache attack and on the performance of the system. The results illustrate that trace-driven attacks based on bus communication are a nonnegligible threat in SoC environments. The results also show that the protection techniques are feasible to implement and that they are able to mitigate the attacks.