Abstract: Multi-Processors Systems-on-Chip (MPSoCs), as a key technology enabler of the new computation paradigm Internet-of-Things (IoT), are currently exposed to attacks. Malicious applications can be downloaded at runtime to the MPSoC, infecting IP-blocks connected to a Network-on-Chip (NoC) and opening doors to perform Timing Side Channel Attacks (TSCA). By monitoring the NoC traffic, an attacker is able to infer the sensitive information, such as secret keys. Previous works have shown that NoC routing can be used to avoid attacks. In this paper we propose GRaNoC, a NoC architecture able to monitor and evaluate the risk of the communication paths inside the NoC. Sensitive traffic is exchanged to minimal low-risk paths defined at runtime. We propose five types of dead-lock free risk-aware routing algorithm and evaluate the security, performance and cost under several synthetic and SPLASH-2 benchmarks. We show that our architecture is able to guarantee secure paths during runtime while adding only low cost and
performance penalties to the MPSoC.

Stichworte: Security; Network-on-Chip; risk path; routing

Dewey Dezimalklassifikation (Liste):
620 Ingenieurwissenschaften


Kongress / Zusatzinformationen: Tallinn, Estonia

Datum der Konferenz: 27.-29.06.2016

Jahr: 2016

Quartal: 2. Quartal

Jahr / Monat: 2016-06

Monat: Jun

Seiten: 6

Revied: ja

Sprache: en

WWW: http://www.recosoc.org/

Occurences:
- Hochschulbibliographie > 2016 > Fakultäten > Elektrotechnik und Informationstechnik > Sicherheit in der Informationstechnik (Prof. Sigl)
- Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2016

entries: