Dokumenttyp: Konferenzbeitrag
Art des Konferenzbeitrags: Textbeitrag / Aufsatz
Autor(en) des Beitrags:
Sepúlveda, Johanna and Flórez, Daniel and Soeken, Mathias and Diguet, Jean-Philippe and Gogniat, Guy
Titel des Beitrags: Dynamic NoC Buffer Allocation for MPSoC Timing Side Channel Attack Protection
Abstract:
Multi-Processors Systems-on-Chip (MPSoCs), as a key technology enabler of the new computation paradigm Internet-of-Things (IoT), are exposed to attacks. Malicious applications can be downloaded at runtime to the MPSoC, infect IPs and open doors to perform timing attacks. By monitoring the Network-on-Chip (NoC) traffic, an attacker is able to spy sensitive information such as secret keys. Previous works have shown that NoC routers can be used to avoid timing attacks. However, such approaches may lead to overall system performance degradation. In this paper we propose SER, a secure enhanced router architecture that dynamically configures the router memory space according to the communication and security properties of the traffic. Timing attacks are avoided by turning the attacker oblivious of the sensitive traffic. We evaluate the security, performance and cost of our approach. We show that our architecture is able to secure paths during runtime while adding only low cost and performance penalties to the MPSoC.
Network-on-Chip, timing, side channel attack

620 Ingenieurwissenschaften

Network-on-Chip, timing, side channel attack (LASCAS)

Florianópolis, Brazil

2016

1. Quartal

2016-03

Mar

ja

en

http://ieee-cas.org/conference/2016-ieee-7th-latin-american-symposium-on-circuits-systems-lasc

- 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: