Security aspects at the compilation level

Tania Richmond, Yoann Marquer, Céline Minh, Nicolas Kiss,
Annelie Heuser and Olivier Zendra

TAMIS team
Univ Rennes, Inria, CNRS, IRISA, France

Abstract. We are involved in the EU Horizon 2020 TeamPlay project[1]. The aim of TeamPlay is to add non-functional properties such as time, energy and security as first class citizens in programs, targeting multi-core heterogeneous platforms (e.g. mobile applications, IoT). At high level, we consider non-functional properties and their expressiveness. We transfer these high level properties down to the low level using the TeamPlay toolchain. At low level, we analyze side-channel vulnerabilities caused by time and power differences and furthermore automatically apply compiler-level countermeasures like equalization or noise addition. To illustrate this work, we rely on the modular exponentiation of RSA.

Keywords: Security properties, execution time, power consumption, side-channel analysis, countermeasures

[1] `https://www.teamplay-h2020.eu/`