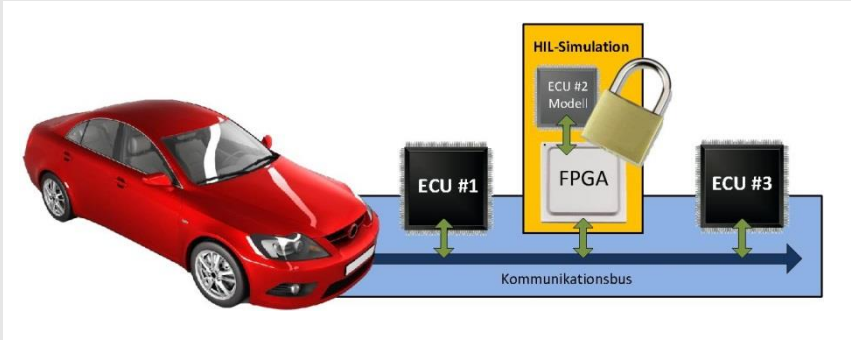
German Research Center for Artificial Intelligence

SecRec

Security by Reconfiguration - Physical security through dynamic and partial hardware reconfiguration

With the ability to dynamically reconfigure protective mechanisms are developed



A FPGA-based simulation model is used for demonstration and verification of the proposed methodologies for reconfiguration based system protection

Motivation

Modern cyber physical systems (CPS) are composed of highly complex building blocks that often need to protect crucial assets such as communication links, implementations and included intellectual property against attacks from the outside world. In this context implementation attacks such as side-channel attacks (SCA) pose a major threat to CPS, since secret information can be extracted non-invasively just by observing side-channel leakages during a operation. The leaked information range from sensitive data to intellectual property (IP).

Project objective:

The goal of the project SecRec is the development of methods and approaches for dynamic reconfiguration-based hardware protection mechanisms against physical attacks. State of the art field programmable gate arrays (FPGAs) provide high-speed reconfiguration interfaces, enabling the reconfiguration of the implemented hardware circuit at run time. The objective of this project is to develop dynamic implementation strategies for FPGAs that provide comprehensive countermeasures against physical attacks, such as reverse engineering (RE), fault injection attacks (FIA) or SCA. Key requirements are formally provable correctness of the dynamic reconfiguration process and efficient implementation of the entire system. Combined local and partial reconfiguration of the system implementation increases the design space significantly. Hence, novel verification methodologies are required to guarantee the same quality and robustness as for designs without support for reconfiguration-based implementation strategies.

Use Case

The manufacturer ETAS provides a Hardware-In-The-Loop (HIL) simulation device. This device contains the model of an electronic control unit (ECU) for automotive applications. This model contains essential IP which must be protected against RE or extraction. Otherwise, providing simulation devices can result in significant financial losses for vendor of the ECU model.

Duration: 10/2016 – 09/2019

Partners:

BOSCH Technik fürs Leben · FZI · MIXED MODE · TUHH Technische Universität Hamburg

Sponsored by:

SPONSORED BY THE Federal Ministry of Education and Research

The project is funded by the Federal Ministry of Education and Research (BMBF), grant no. 16K1S0606K.

Contact:
DFKI GmbH, location Bremen
Department Cyber-Physical Systems
Project leader: Prof. Dr. Ing. Tim Erhan Güneysu
Phone: +49 234 - 32 - 24626
E-mail: Tim_Erhan.Gueneysu@dfki.de
Website: www-cps.hb.dfki.de/research/projects/SecRec