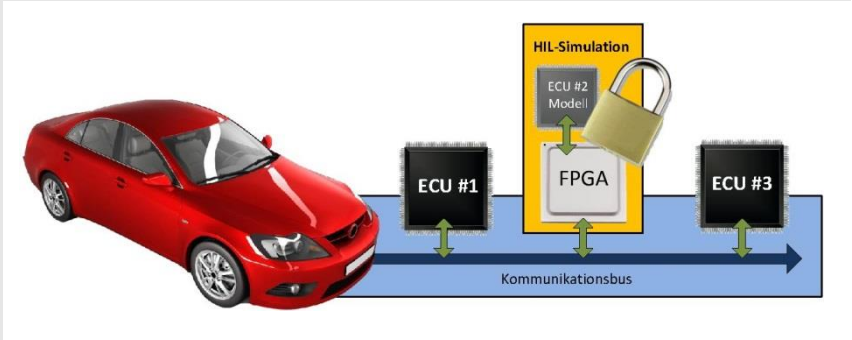
Deutsches Forschungszentrum für Künstliche Intelligenz GmbH

SecRec

Sicherheit durch Rekonfiguration – Sicherheit auf Schaltungsebene durch dynamische partielle Rekonfiguration

Mit der Fähigkeit zur dynamischen Rekonfiguration werden Schutzmechanismen entwickelt



Am Beispiel sicherheitskritischer FPGA-basierter Simulationsmodelle werden die entwickelten Schutzmaßnahmen für Hardware-Implementierungen demonstriert und verifiziert.

Motivation

Moderne Cyber-Physische Systeme (CPS) bestehen aus einer Vielzahl komplexer Grundbausteine. Diese müssen gegen Angriffe von außen geschützt werden. Hierbei stellen Seitenkanalangriffe eine große Gefahr dar, da durch sie geheime Informationen nicht-invasiv aus CPS extrahiert werden können. Die durchgesickerten Informationen reichen von sensiblen Daten bis zu geistigem Eigentum.

Projektziel

Ziel des Projekts SecRec ist es, wirksame Schutzmaßnahmen für CPS durch dynamische und lokale Rekonfiguration zu entwickeln, welche die Systeme gegen Angriffe auf Schaltungsebene schützen. Moderne Field Programmable Gate Arrays (FPGAs) bieten bereits leistungsfähige Werkzeuge zur Rekonfiguration von Hardware-Schaltungen. Die konkrete Realisierung einer Schaltung in FPGAs kann so zur Laufzeit verändert werden. Aus Sicht von Angreifern wird die Komplexität der Implementierung dadurch drastisch erhöht, was Angriffe auf derart geschützte Systeme erheblich erschwert. Im Projekt werden dynamische Implementierungsstrategien für FPGAs entwickelt, die umfassende Gegenmaßnahmen gegen physikalische Angriffe wie Reverse Engineering, Fehlerinjektionsangriffe oder Seitenkanalangriffe bieten. In diesem Kontext sind Nachweise der Korrektheit jeder Rekonfiguration sowie der Effektivität und Effizienz der Implementierung von großer Bedeutung. Mithilfe neuer Verifikations- und Testmethoden wird gezeigt, dass die durch Rekonfiguration geschützten Systeme ebenso korrekt und robust arbeiten wie klassische Systeme ohne derartigen Schutz.

Anwendungsfall

Als Anwendungsfall dient das Simulationsmodell des Herstellers ETAS für ein modernes Steuergerät aus dem Automobilbereich. Das Modell enthält wertvolles geistiges Eigentum, das vor Angriffen wie Reverse Engineering oder Extraktion geschützt werden muss, da diese üblicherweise einen erheblichen finanziellen Schaden für das Unternehmen nach sich ziehen.

Projektlaufzeit: 10/2016 – 09/2019

Partner:

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

Gefördert durch:

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Das Projekt wird gefördert vom Bundesministerium für Bildung und Forschung (BMBF), Förderkennzeichen 16K1S0606K.

Kontakt:
DFKI GmbH, Standort Bremen
FB Cyber-Physical-Systems
Projektleiter: Prof. Dr. Ing. Tim Erhan Güneysu
Telefon: 0234 - 32 - 24626
E-Mail: Tim_Erhan.Gueneysu@dfki.de
Internet: www-cps.hb.dfki.de/research/projects/SecRec