Hierarchical Integrity Checking in Heterogeneous Vehicular Networks
Dominik Püllen, Nikolaos Athanasios Anagnostopoulos, Tolga Arul & Stefan Katzenbeisser

Introduction and Motivation

- Human drivers will be slowly replaced by intelligent machines relying on sensor input and sophisticated algorithms.
  - UNICARagil [1] vehicles
  - SAE level 5 [2] road vehicles
- Safety must be guaranteed to gain acceptance for autonomous vehicles in society.
- The vehicle’s integrity state has to be verifiable to ensure a safe driving state:
  - hardware integrity
  - software integrity

Goal: Compute integrity identifiers to represent the vehicle’s integrity state

Abstract Vehicular Structure

- Derivation of an integrity identifier $i_{\text{VEHICLE}}$ indicating the overall vehicle’s integrity state
- The vehicle is logically divided into three hierarchical levels.

Hierarchical Integrity Checking

An identity identifier $i_{\text{component}}$ represents the integrity state of a specific component.

An integrity measurement of a component is the verification of its valid hardware and software state.

Characteristics of $i_{\text{VEHICLE}}$:

- It should give instant feedback about the vehicle’s integrity usable by third parties
- It should be made available to third parties such as car manufacturers and authorities.
- It should incorporate the integrity measurements of low-end devices (e.g. sensors) and computational powerful units (e.g. environment perception ECU) creation of a secure key to eventually perform hardware and software attestation

Challenges and Opportunities:

- Platform Heterogeneity:
  - low-end devices: Physical Unclonable Functions (PUFs)
  - inherent key derivation based on hardware characteristics
  - high-end devices: Trusted Platform Modules (TPMs)
  - vendor-generated secure key stored in tamper-proof chip
- Hierarchy:
  - compute identifiers in a distributed way to more reliably distinguish between safety-critical components
- Identifier Distribution:
  - V2X communication
  - blockchain

Challenge-Response Game:

Verifier (e.g. authority) $n$ Prover (vehicle)

On each hierarchy layer:

- integrity measurements of components
- encryption of $n$ with the output of the integrity measurements, resulting in integrity identifiers
- recursive collection, hashing and propagation of integrity identifiers to the upper layer, finally resulting in $i_{\text{VEHICLE}}$

- compare the received $i_{\text{VEHICLE}}$ with the value calculated in advance

References
