Towards an Integrated In-Vehicle Isolation and Resilience Framework for Connected Autonomous Vehicles

Khaled Mahbub, Mohammad Patwary, Antonio Nehme
Birmingham City University
Birmingham, United Kingdom
Email:{firstname.lastname}@bcu.ac.uk

Marc Lacoste, Sylvain Allio, Yvan Rafflé
Orange Labs
France
Email:{firstname.lastname}@orange.com

BIRMINGHAM CITY University

IARIA

About the Presenter

Antonio Nehme holds a BSc in Computer Science with a minor in Mathematics from the Lebanese American University and a PhD in Cyber Security from Birmingham City University. Dr Nehme is currently working on the project "Isolation and Resilience in Networks of Autonomous Vehicles" at Birmingham City University. His research interests include access control and online consents, auditing and non-repudiation, data privacy and security, cloud security, risk management, digital forensics, Blockchain and IoT.

Isolation and Resilience in Networks of Autonomous Vehicles

Autonomous Vehicles require:

- In-vehicle connectivity between sensors, ECUs, OBUs
- Vehicle to Vehicle connectivity
- Vehicle to Roadside Infrastructure and broadband cloud connectivity

More Connectivity
➔
Larger Attack Surface

In-vehicle communication:

- Diversity of Equipment
- Diversity coding practices
- Unrestricted on-board communication

Network and Equipment level
➔
Possibility of Compromise

In-Vehicle Isolation and Resilience

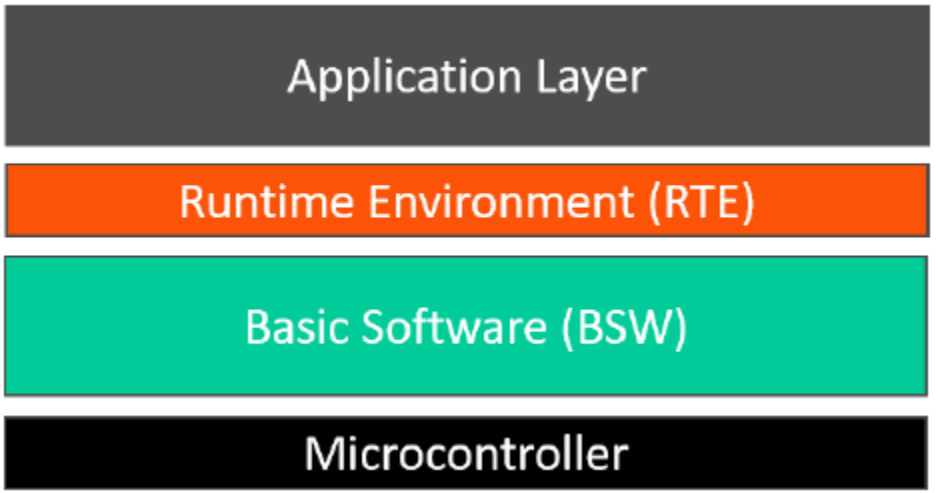
Tackling security challenges of In-Vehicle Networks:

- Standards to tackle diversity➔ AUTOSAR standard
- Isolation for tackle integrity and confidentiality➔ Trusted Execution Environment
- Security rules to monitor the In-Vehicle network➔ protection from injection and replay attacks
- Functional Rules ➔ detect abnormalities of behaviour
- Side Channel➔ revealing attempts of side channel attacks

Certification:

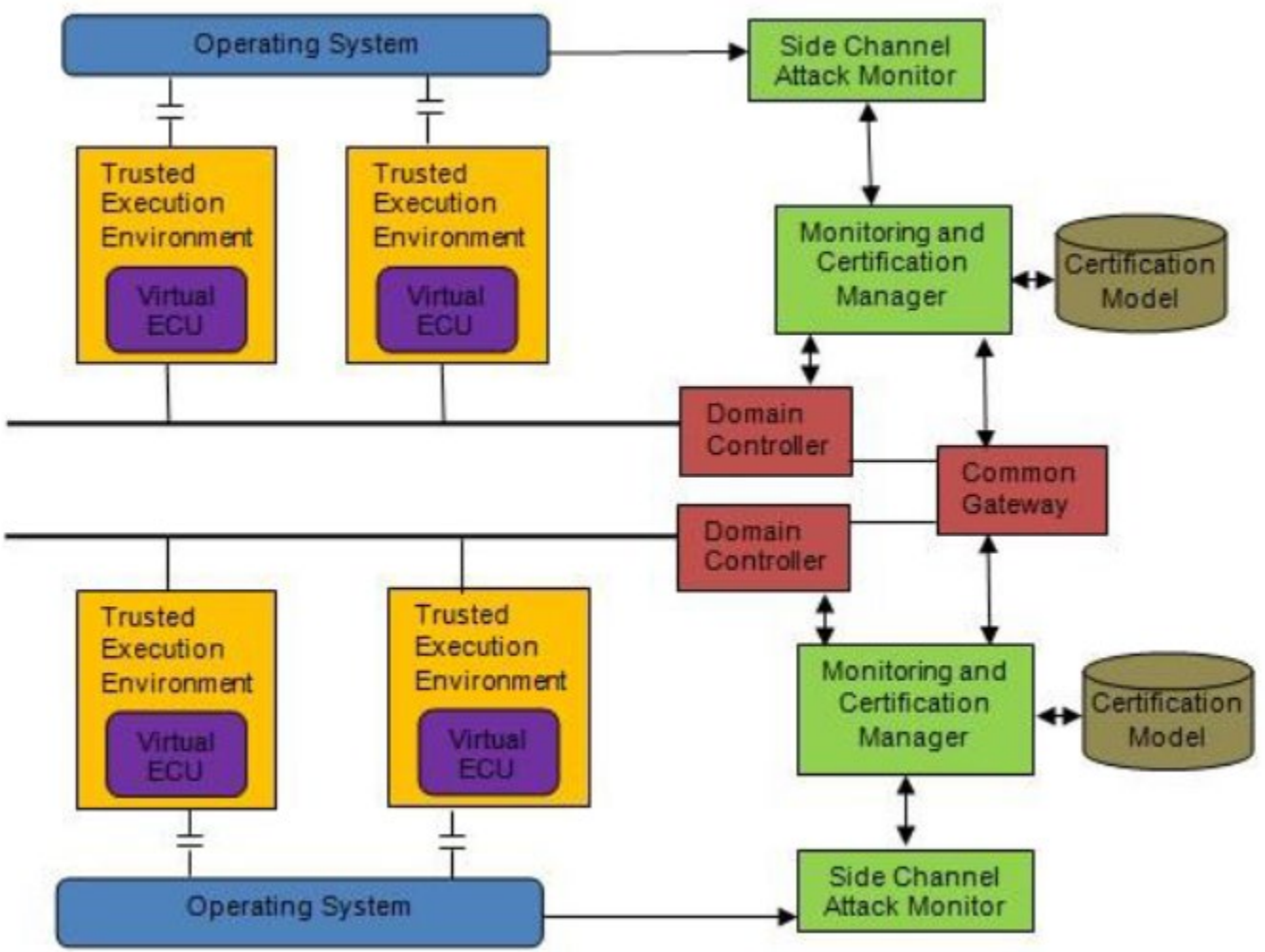
- Certificate reflecting the health of the in-vehicle network
- Details for every target of monitoring (security and functional)

Overview of AUTOSAR

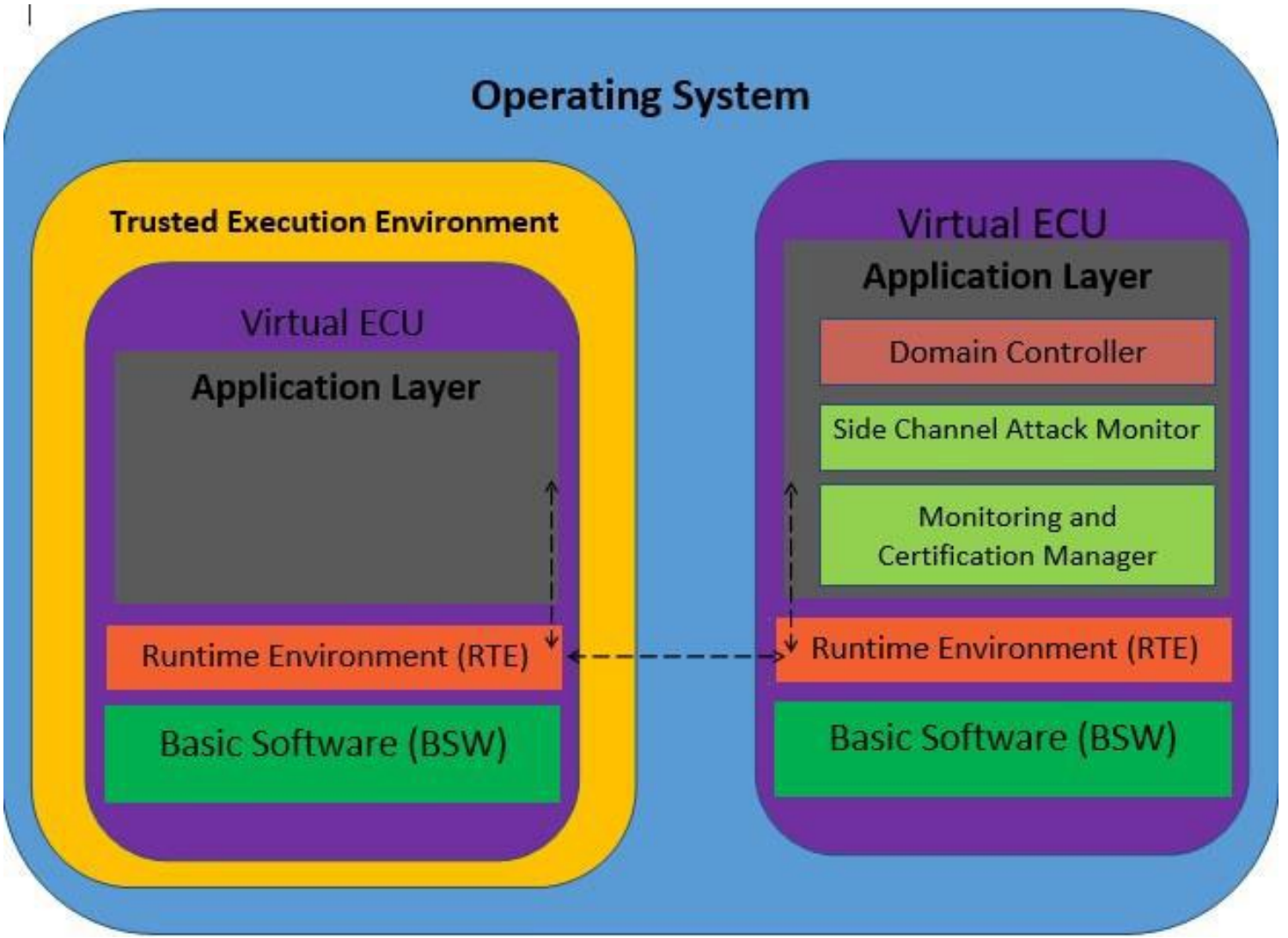


- Application Layer: Software components of the ECU
- Runtime Environment: Communication between ECUs and between the Application and BSW
- Basic Software: Includes system functionalities (Operating system, drivers, memory services) and interfaces the Microcontroller.

Reference Architecture of Isolation and Resilience Framework



Mapping Our Framework to AUTOSAR



Outlook and Future Work

- Adopting an open source implementation of AUTOSAR for Virtual ECUs
- Using CLIPS Rule engine for security and functional rules
- Using Open Enclave for TEE
- Using JSON for the representation of certificates
- Simulating an In-Vehicle network and evaluating the framework