Overall Project Technical Review – 4 Pillars

Peter Hofmann (DT-Sec)

OEM Workshop

Online – November 16 2021

Agenda

Agenda

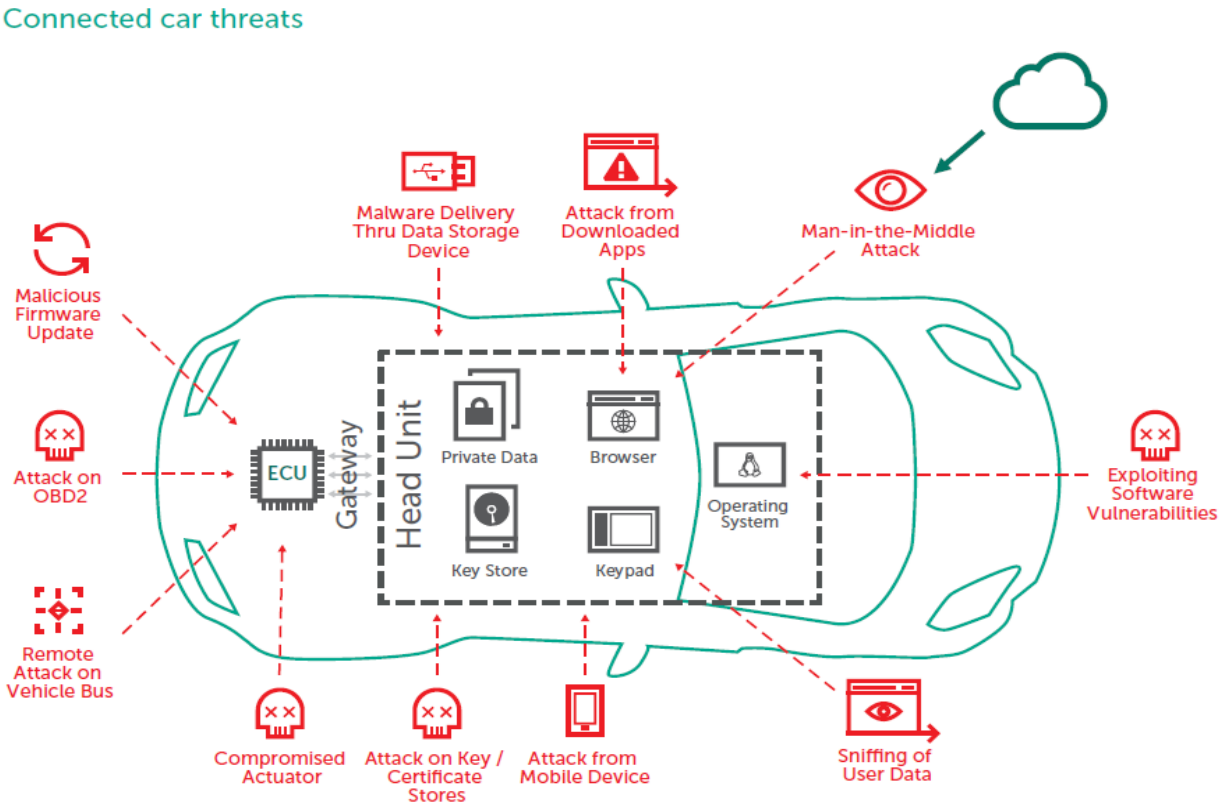
- Motivation – threats to connected vehicles
- CARAMEL project overview
- The anti-hacking device
- Pillar 1: Attacks against sensors
- Pillar 2: Attacks against the connected vehicle
- Pillar 3: Attacks against the eCharging infrastructure
- Pillar 4: Korean partners: Remote Controlled vehicle, Cyber security module based on AI, ML-based intrusion detection
- Conclusions and next steps

Motivation

Attack surfaces

A modern car is a data center on wheels with a multitude of attack surfaces:

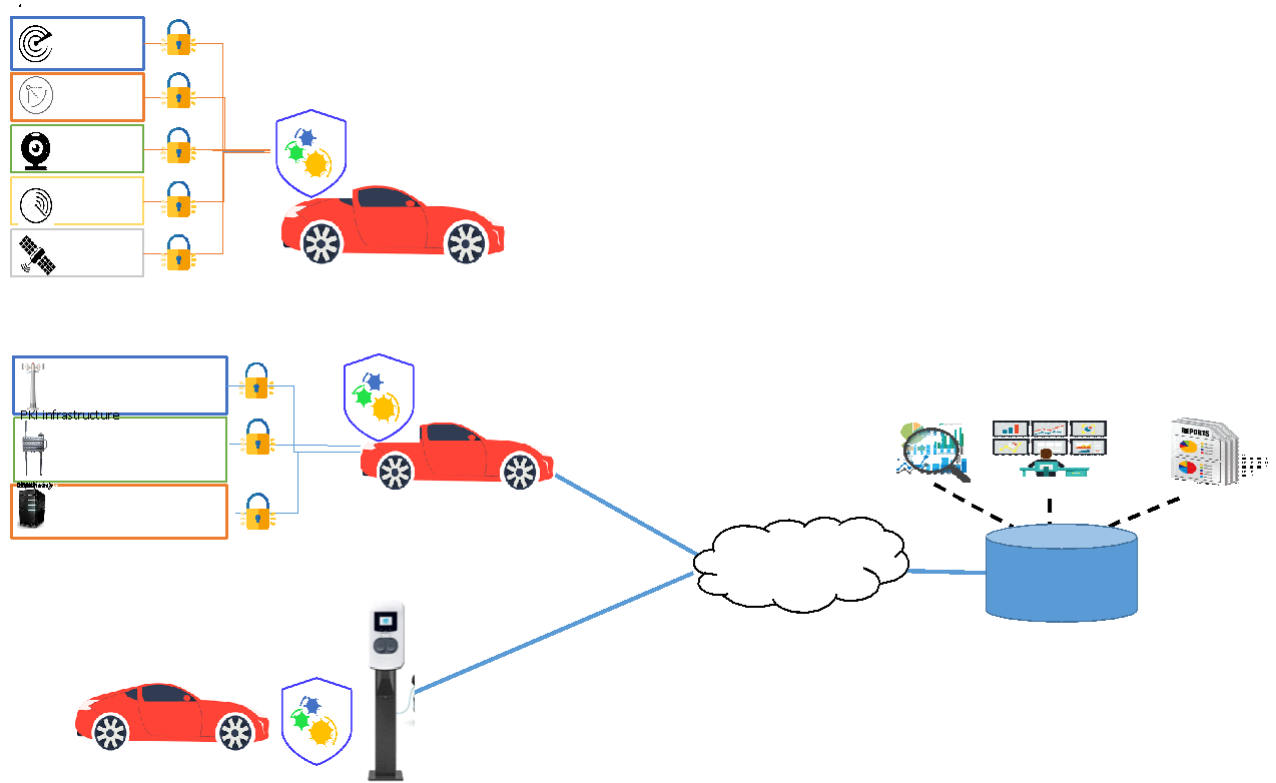
- Entertainment system
- Internal buses
- Sensors
- Cloud interfaces
- Interfaces to other vehicles and the road-side infrastructure (V2X)



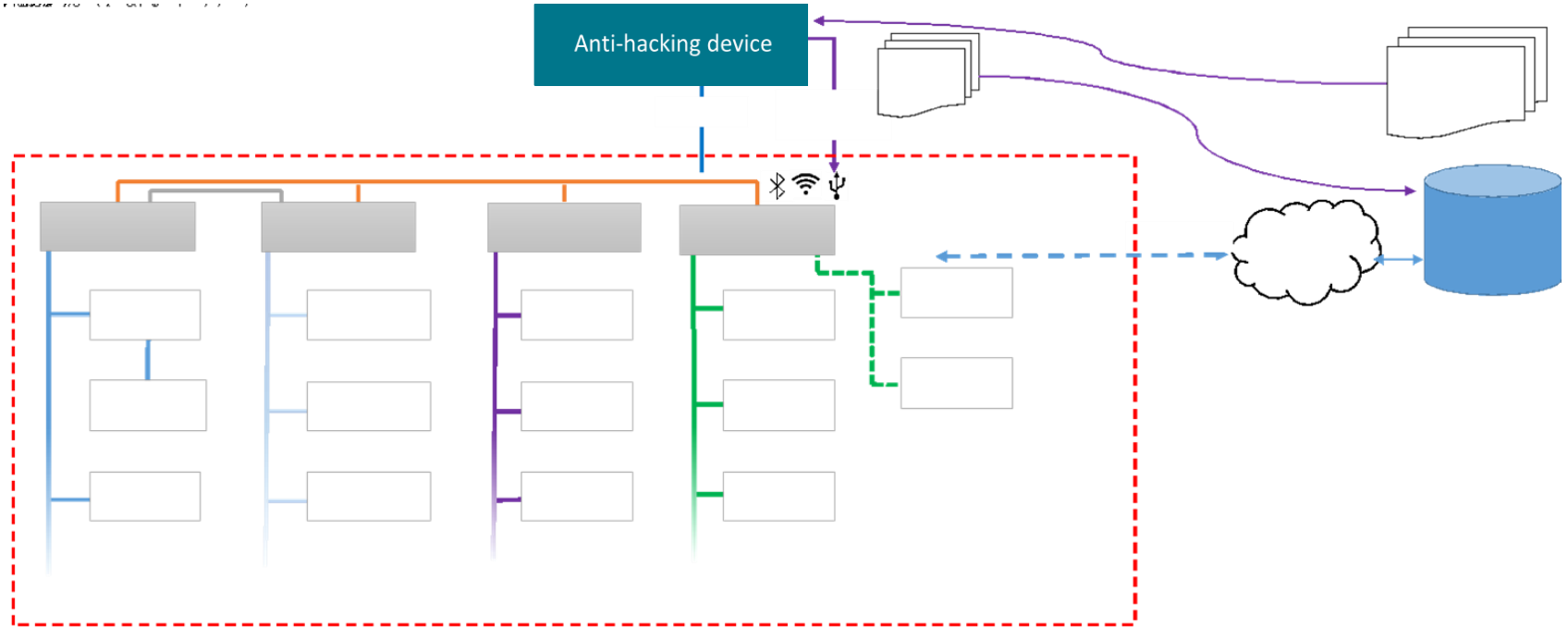
High-level overview

CARAMEL pillars

- Pillar 1
  - Attacks against sensors
- Pillar 2
  - Attacks against V2X infrastructure (forging of messages, vehicle track)
  - GPS spoofing
  - OBU compromise
- Pillar 3
  - eCharging manipulation
- Pillar 4: KR partners
- Common element:
  - Anti-hacking device



The Anti-hacking Device

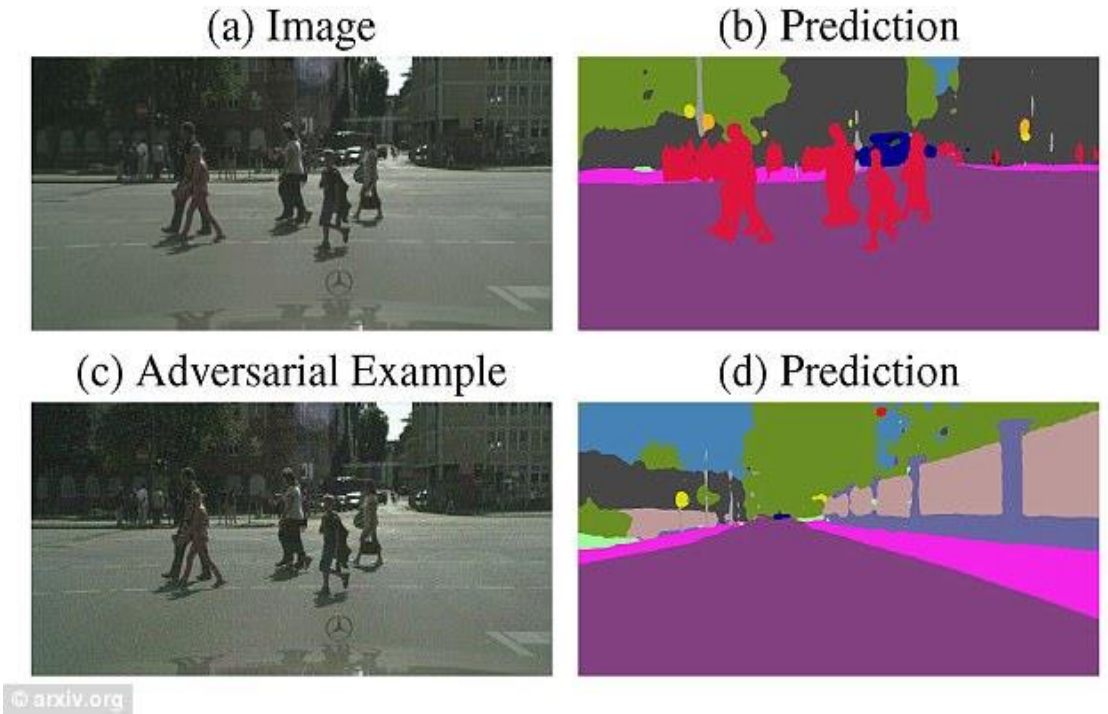


- **Passive intrusion detection device** in the car that receives messages from other components:
- **Connected** to vehicle's internal busses
- Should **not** present an **attack surface** on its own

Pillar 1: Attacks Against Sensors

Adversarial

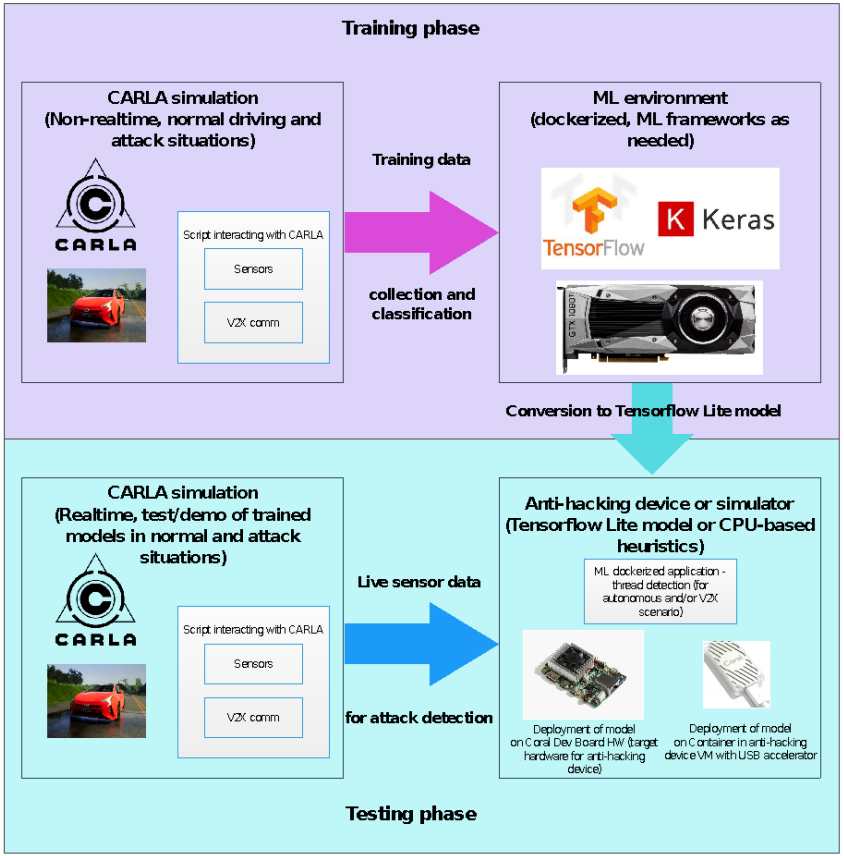
- Autonomous vehicles use perception modules for object localization such as **object detectors** and object segmentation to generate an understanding of the vehicle's environment
- Deep learning neural networks (DNN) are known to be **vulnerable to adversarial examples** (AE)
- The attack can be physical by introducing **physical manipulations** to the actual environment that are often imperceptible to people
- The attack can also be a **cyberattack on the sensor** systems in the car
- Attackers use **generative adversarial networks** (GAN) to generate the attack patterns automatically



Pillar 1: Detection of Sensor Attacks

Attack against camera – defaced traffic signs

- Training phase:
  - Algorithmically generate defaced traffic signs
  - Use CARLA simulation environment to generate labeled image data from simulated sensor
  - Create Tensorflow model from labeled data
  - Convert for use on anti-hacking device
- Testing/demonstration phase:
  - Algorithmically or manually create defaced signs
  - Send data to anti-hacking device (Coral Dev Board with Tensorflow Edge TPU)
  - Generate alerts and send to SOC



Pillar 2: Attacks Against Connected Cars

V2X infrastructure

Secure multi-technology OBU:

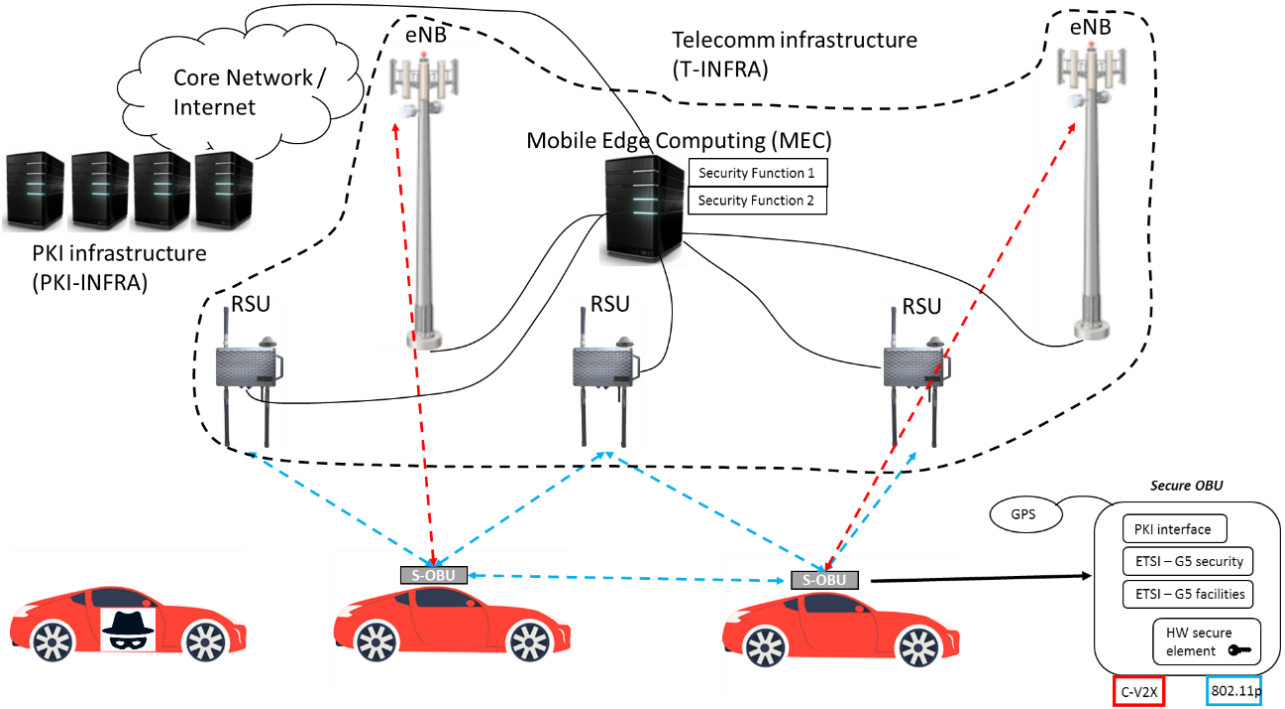
- ❑ **802.11p and C-V2X**
- ❑ Secure ETSI-G5 messaging
- ❑ Secure HW element to store key material

Prototype radio infrastructure:

- ❑ eNB and RSU,
- ❑ MEC server able to host **virtual security functions** and IEEE 802.11p/C-V2X **interoperability** functions

Prototype V2X-enabled PKI:

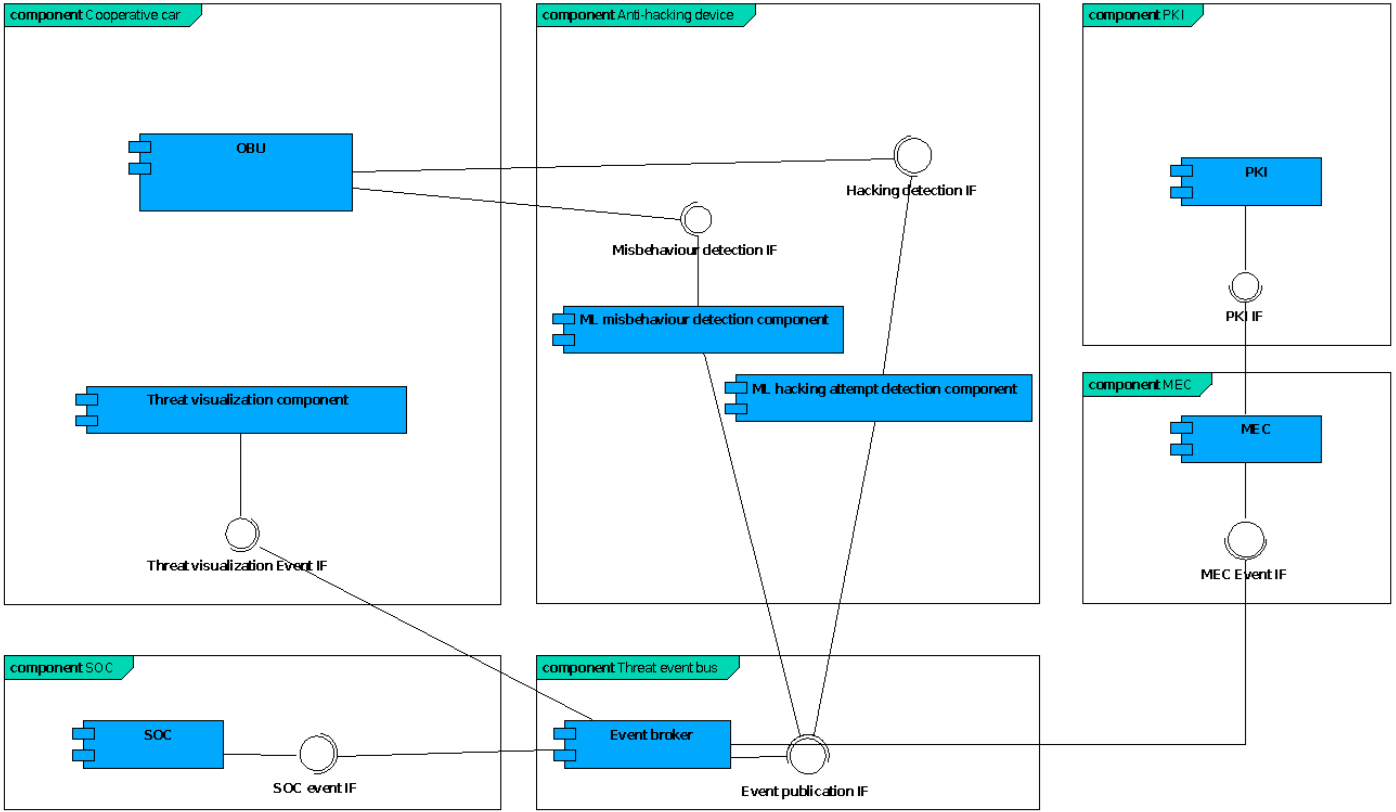
- ❑ **V2X pseudonym certificates**



Pillar 2: Attacks Against Connected Cars

V2X attack

- Attack on V2X messages
- Detected by anti-hacking device
- Event passed to
  - On-board display
  - MEC/PKI for certificate revocation
  - SOC for alerting



Pillar 3: Attacks Against eCharging

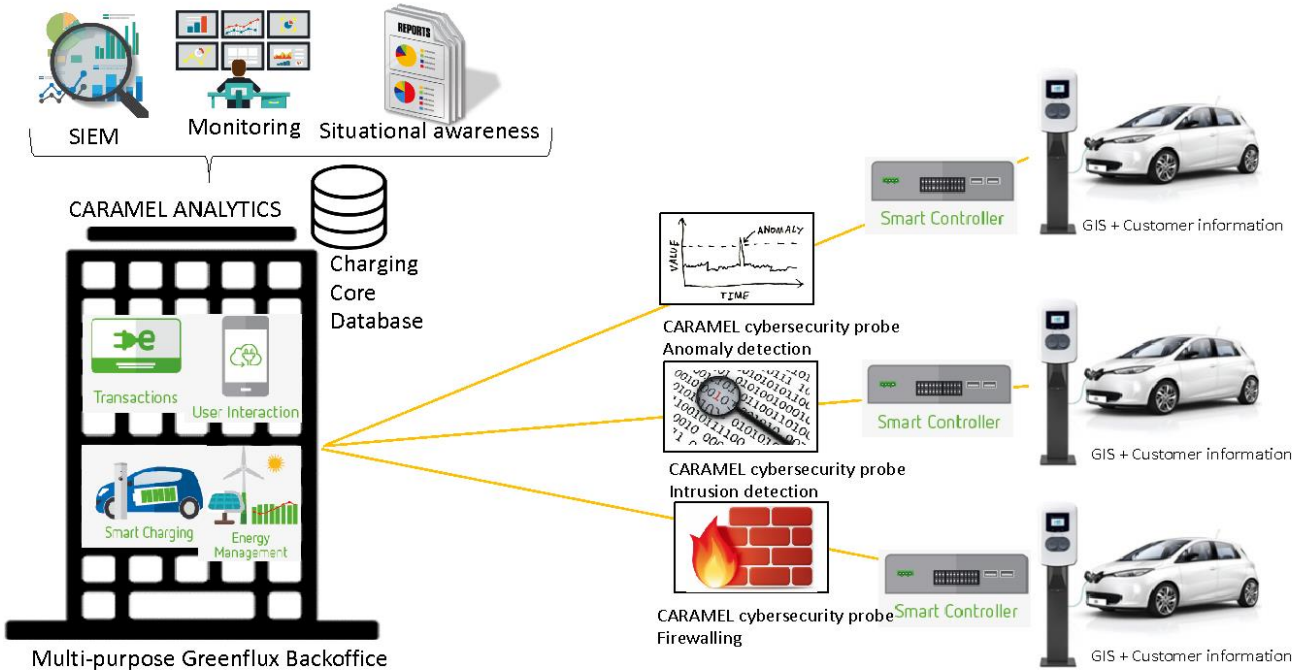
Attacks and mitigation

Possible attack vectors:

- Attacks against the smart controller in the charging point
- Concerted attack against the electric grid

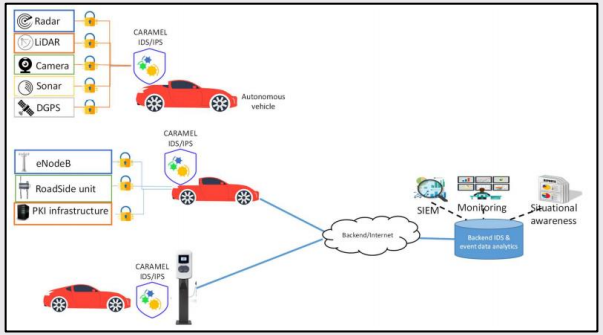
Mitigations in the project:

- Focus on grid attacks
- ”anti-hacking device in the cloud”: Use machine learning to detect attack patterns from backoffice data

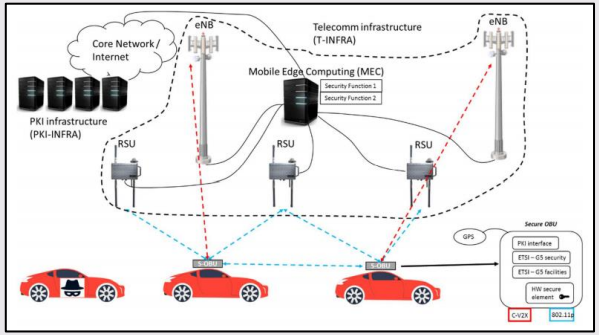


Pillar 4: Attacks Against eCharging

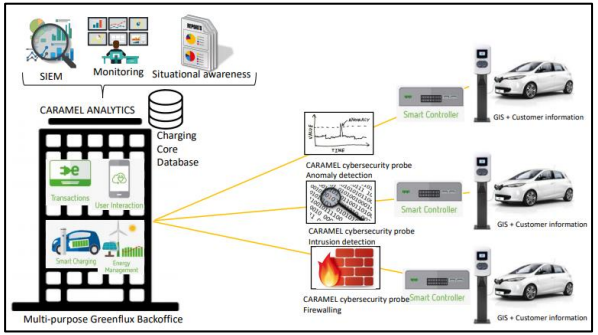
Korean partners: KATECH, ETRI, MOBIGEN



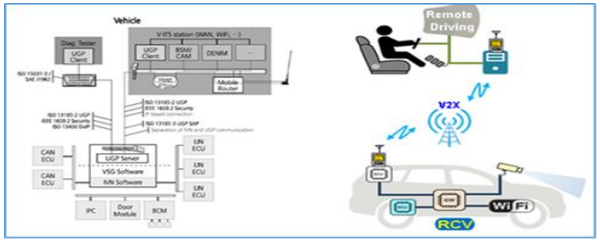
< CARAMEL high-level architecture>



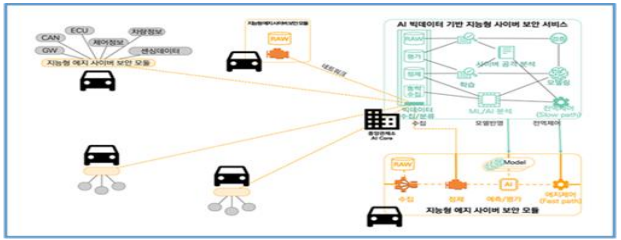
< CARAMEL vision on secure multi-technology V2X connectivity >



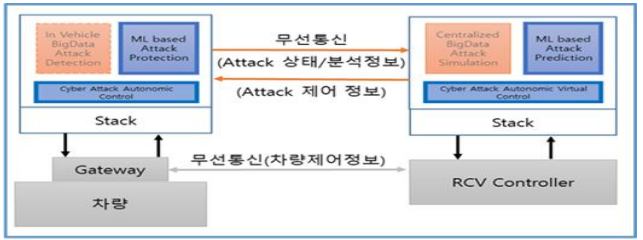
< CARAMEL protection mechanisms and countermeasures for attacks to PEVs >



Vehicle Gateway and Remote Controlled Vehicle



Automotive cyber security module based on AI (AI Edge)



ML based intrusion detection and estimation algorithm

Thank you for your attention!