



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Automotive Cybersecurity

Pozsonyi Tamás
Nagy Róbert

Tesla Model 3's infotainment unit hacked in minutes in competition

3rd April 2023, 14:56 by Rahul Nagaraj



Hyundai and Kia agree to \$200 million settlement over TikTok car theft challenge

Car-theft season is here; TikTok challenge targeting Hyundai, Kia cars makes it worse than ever



- Main concept
- Technologies and Protocols
- The project
- VSOC
- Security

Presentation topics

Objectives:

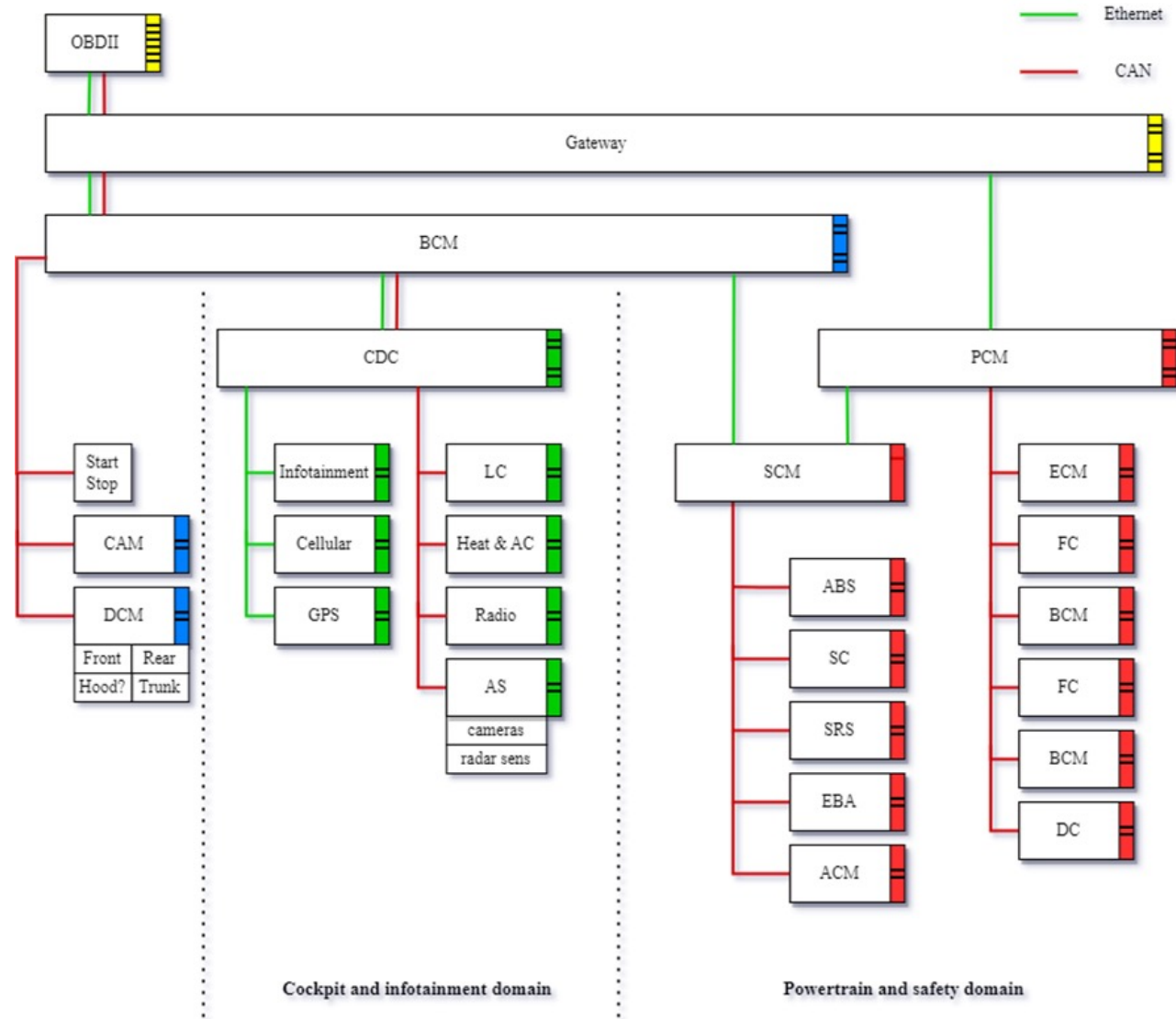
- Connect multiple boards to mimic ECUs
- Set up the protocols
- Penetration test it
- Log traffic to VSOC
- Try to find attacks

Main Concept



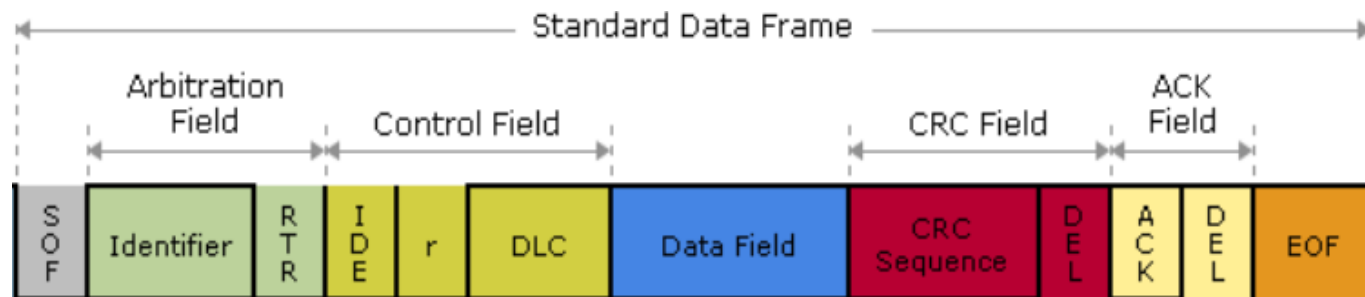
ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Technologies and Protocols



What is it?

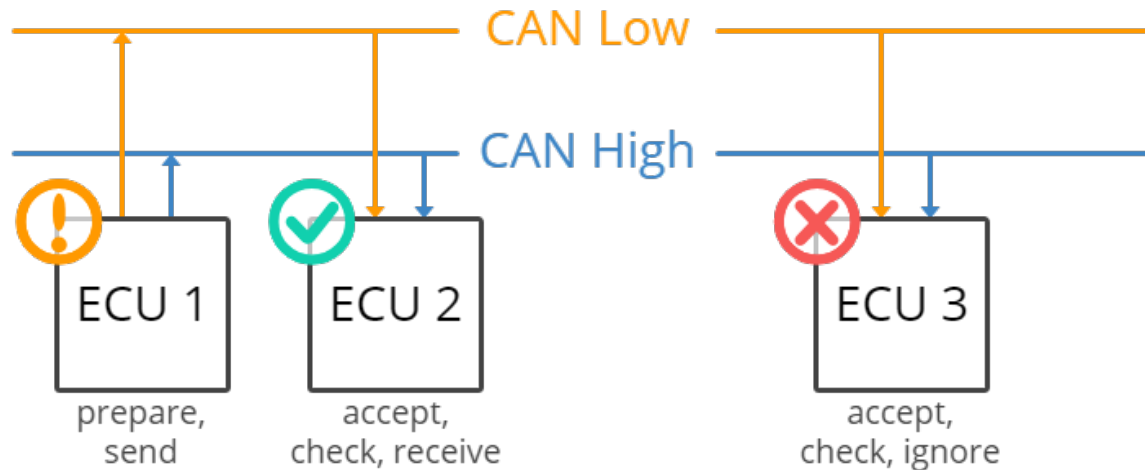
- „Controller Area Network”
- Collision Avoidance
- Lowest ID Highest priority
- Similar to the nervous system
- Message-based protocol



CAN Protocol

Why use it?

- Simple, low cost
- Efficient, scalable/flexible and reliable
- Centralized, broadcast architecture
- Error detection



CAN Protocol

What is Automotive Ethernet:

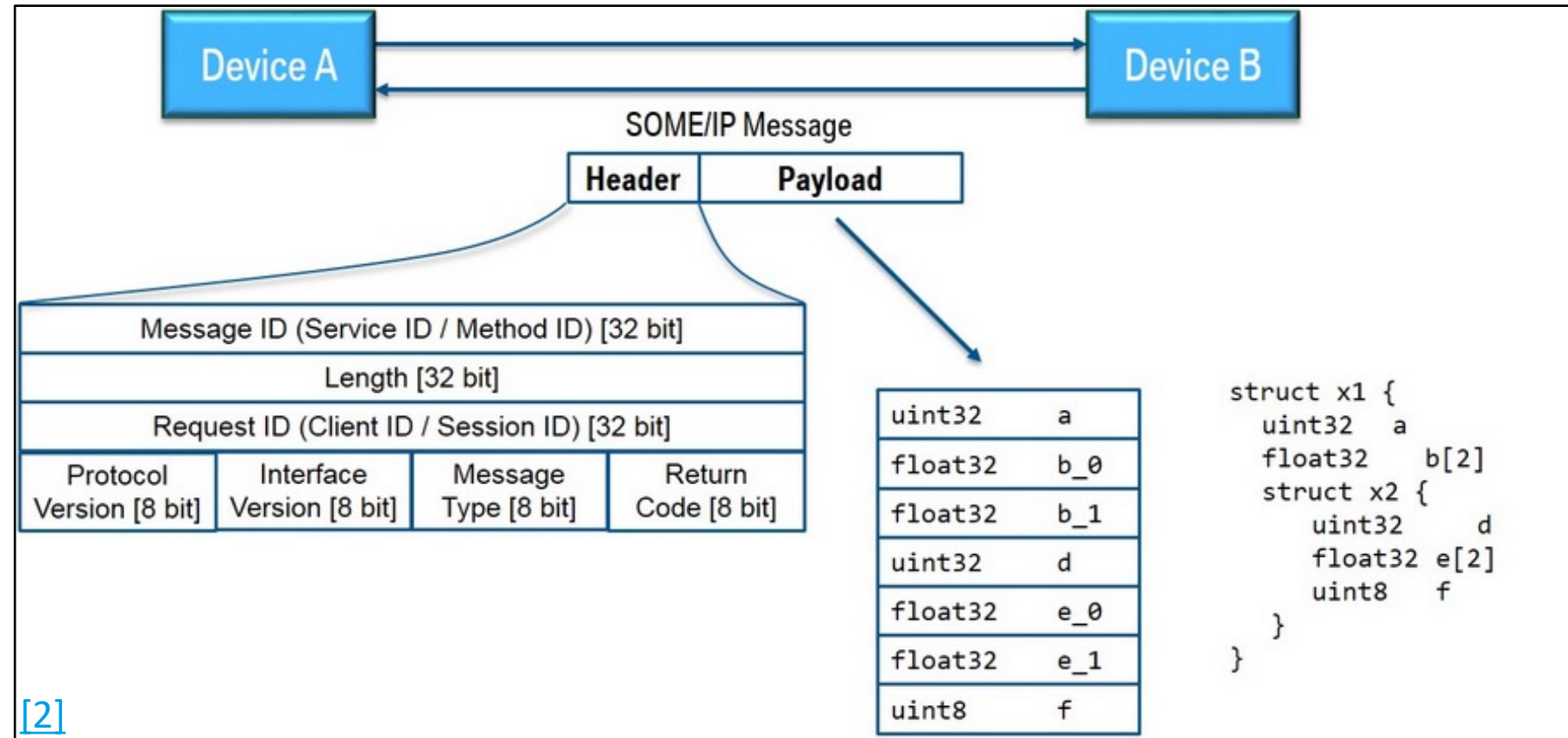
- Ethernet for Cars
- Higher data rate
- Broader bandwidth
- Compatible with other network protocols
- Non-real time applications, infotainment and diagnostics

Automotive Ethernet

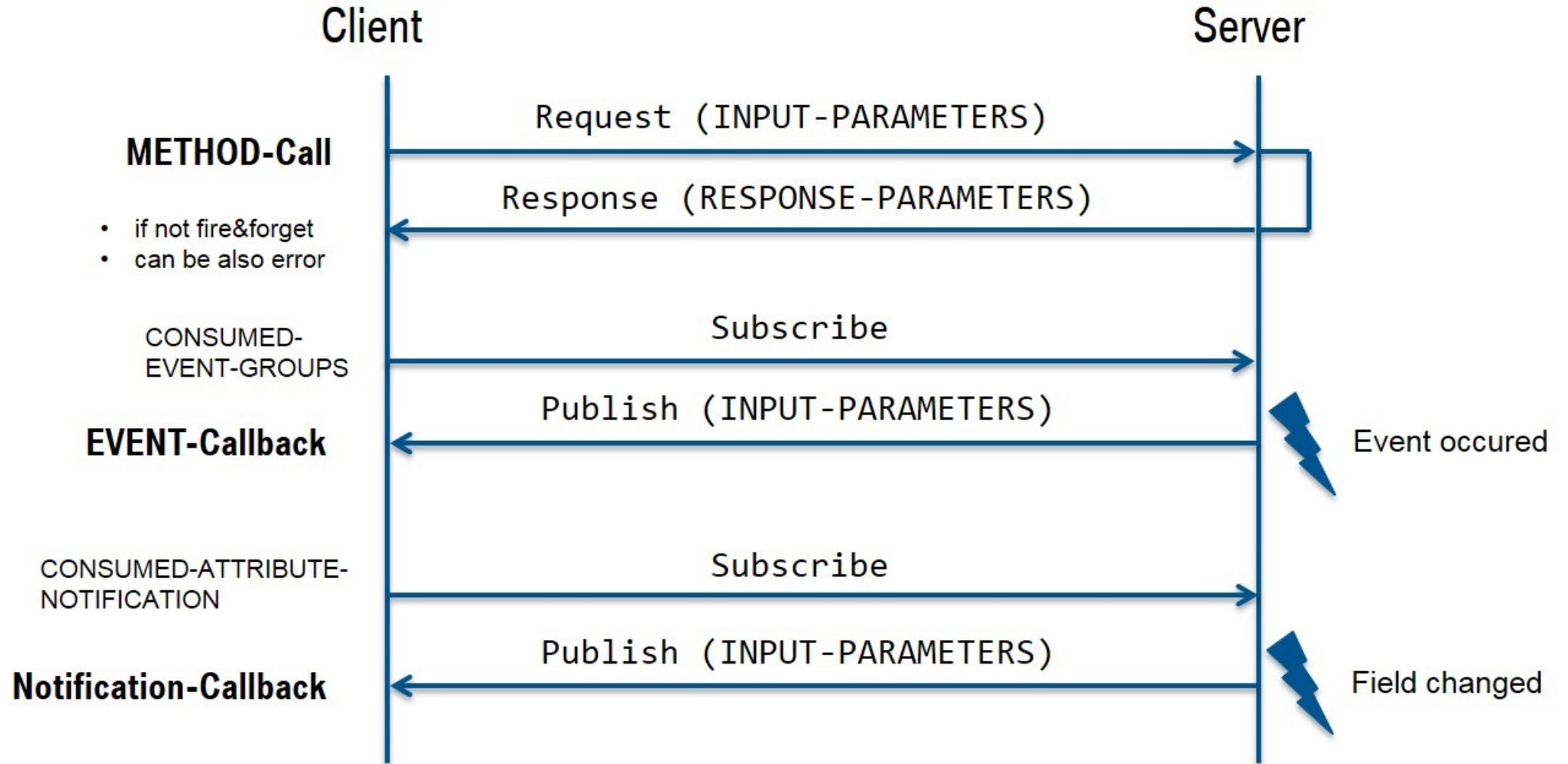
Scalable service Oriented MiddlewarE over IP (SOME/IP) protocol:

- Service discovery
- Publish/Subscribe
- Multicast
- Message framing
- Low overhead for trasmission

SOME/IP
protocol



SOME/IP Packet



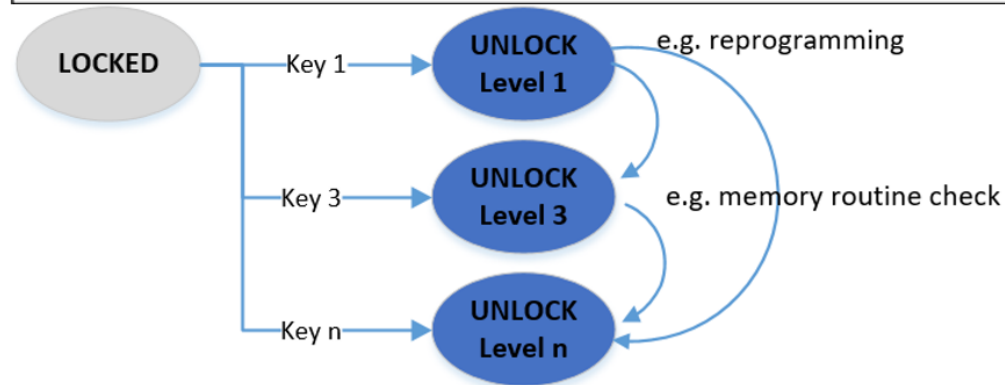
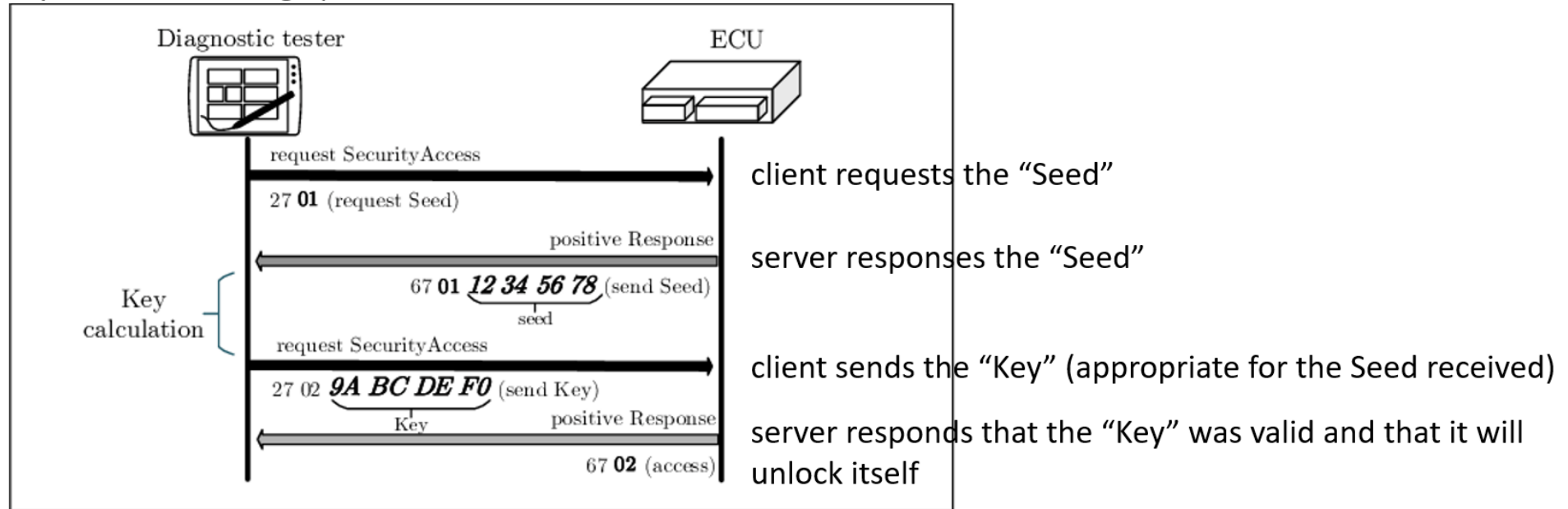
SOME/IP Communication

Unified Diagnostics Services protocol

- Offboard diagnostics
- Reprogramming ECUs
- After sale servicing
- Different to OBD

UDS

Symmetric challenge process



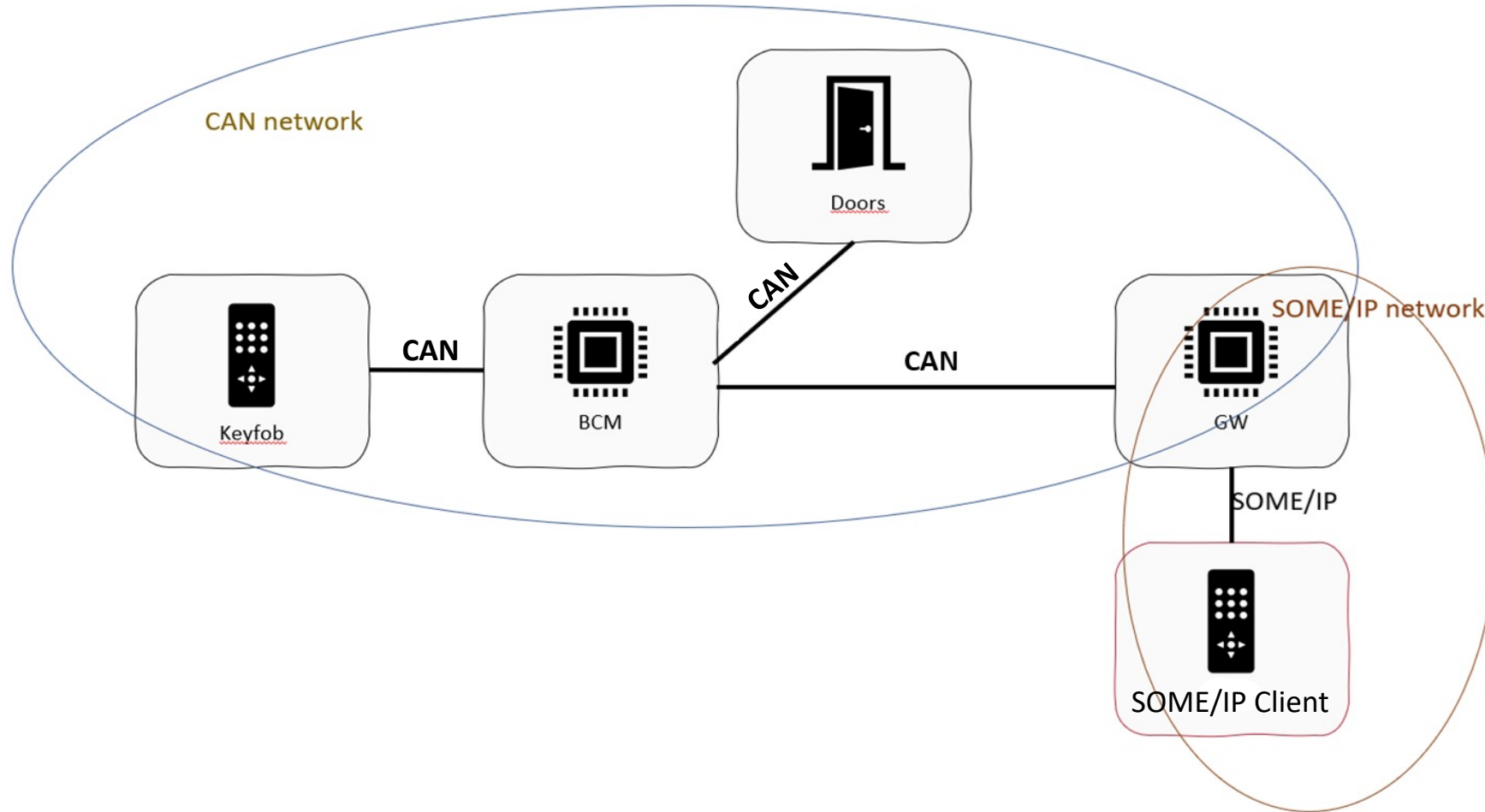
Security access is not available in default session

- Change to extended session, then change to the required security level to access critical services.



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

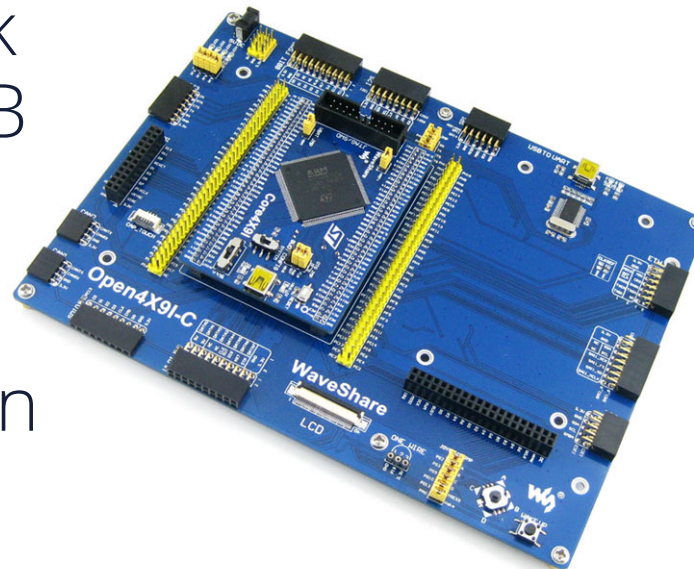
The project

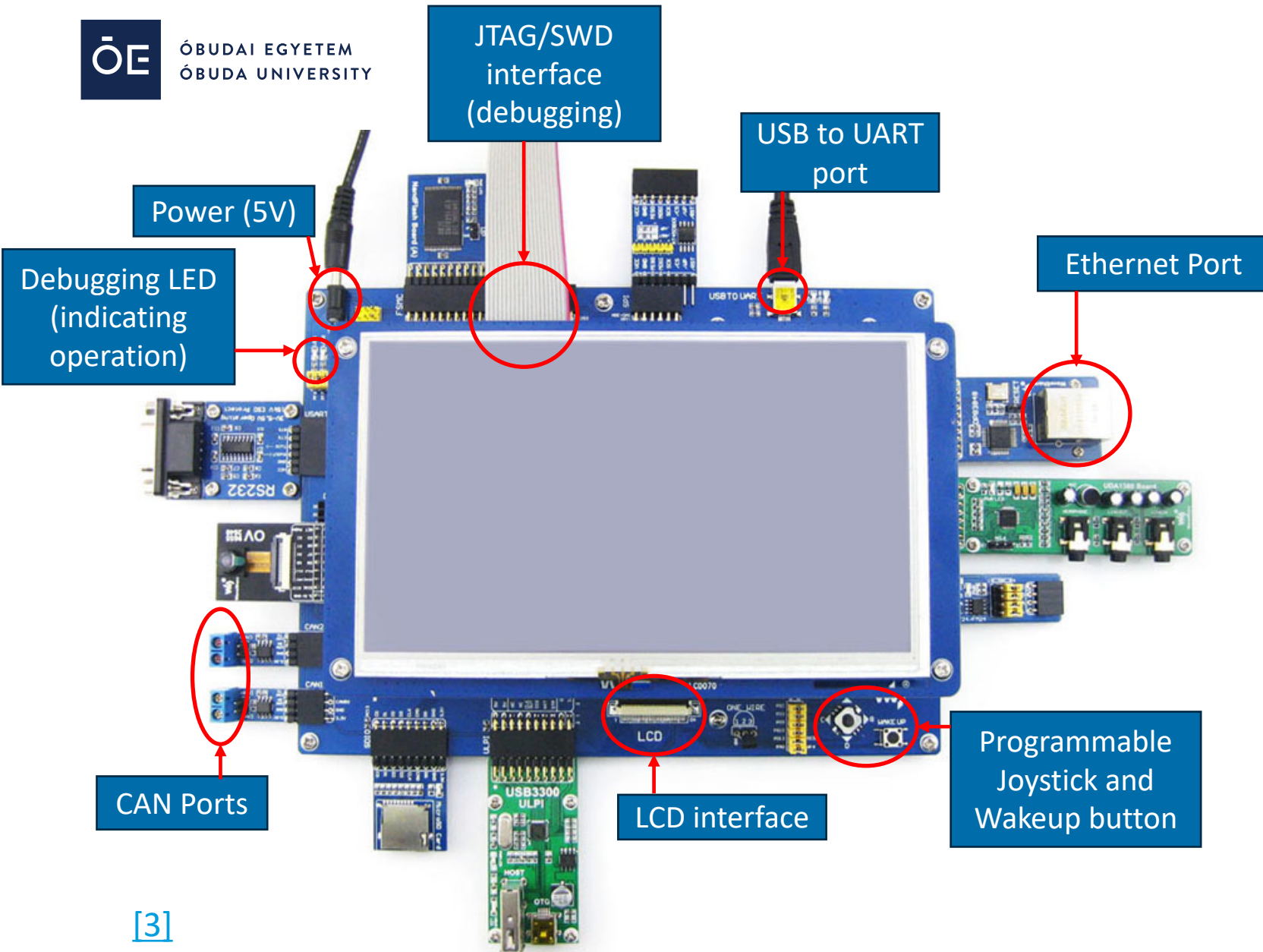


Our Architecture

STM32 Series Microcontroller

- Operating Frequency of 180MHz
- Controller Area Network (CAN), Ethernet and USB ports
- LCD screen
- Input Joystick and button





Board accessories and ports



- CAN communication
- Processing user input
- SOME/IP implementation
- Recognised as an end device on networks
- LCD responds to input and shows messages
- UART communication
- Compatible with other boards

Our progress



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Security

Known attacks:

- Sniffing
- Denial of Service
 - Network
 - ECU
- Spoofing
 - Masquerade
 - Replay

Attack
types



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

VSOC

The way it should work:

- Collect logs from the board
- Analyze traffic
- Look for trends and anomalies
- Alert if suspicious

VSOC





ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Thank you for your attention!

Sources:

- [1] <https://github.com/COVESA/vsomeip/wiki/vsomeip-in-10-minutes#first>
- [2] <https://nvdungx.github.io/unified-diagnostic-protocol-overview/>
- [3] <https://www.waveshare.com/open429i-c-standard.htm>