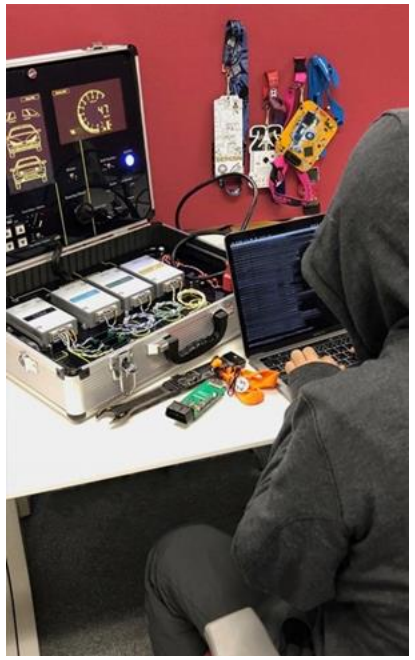
PASTA: Portable Automotive Security Testbed with Adaptability

Tsuyoshi Toyama, Takuya Yoshida, Hisashi Oguma, Tsutomu Matsumoto

Who are we?



Tsuyoshi Toyama

TOYOTA INFOTECH

Takuya Yoshida

TOYOTA INFOTECH

Toyota InfoTechnology Center Co.,Ltd
https://www.toyota-itc.com/en/

Hisashi Oguma

TOYOTA INFOTECH

Tsutomu Matsumoto

YNU YOKOHAMA National University

Yokohama National University
http://er-web.jmk.ynu.ac.jp/html/MATSUMOTO_Tsutomu/en.html

Agenda

- Background of vehicular security
- What is PASTA ?
- Demo
- Use cases
- Roadmap
- Take away

Background

- Lots of ECUs are in a vehicle to realize comfortable driving.
- ECUs interact with other ECUs, sensors, and actuators using CAN protocol, etc.
- CAN Protocol was developed with no concern about cyber security attacks.

Vehicle hacking is real threat

- July 2015, two hackers presented that Jeep Chrysler can be remotely controlled.
  - Controlling wipers, audio system, steering wheels, etc. of a running car.
  - As a result, Chrysler recalled 1.4 million vehicles.

Remote Exploitation of an Unaltered Passenger Vehicle

Dr. Charlie Miller (cmiller@openrce.org)
Chris Valasek (cvalasek@gmail.com)

August 10, 2015

WIRED

ANDY GREENBERG SECURITY 07.24.15 12:30 PM

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

CNN Money Business Markets Tech Personal Finance Small Business Luxury stock tickers

Cyber-Safe

Chryslers can be hacked over the Internet

Recommend 6.3k

By Jose Pagliery @Jose

Most Popular

Whole Fooc cheaper tha bottles of as water

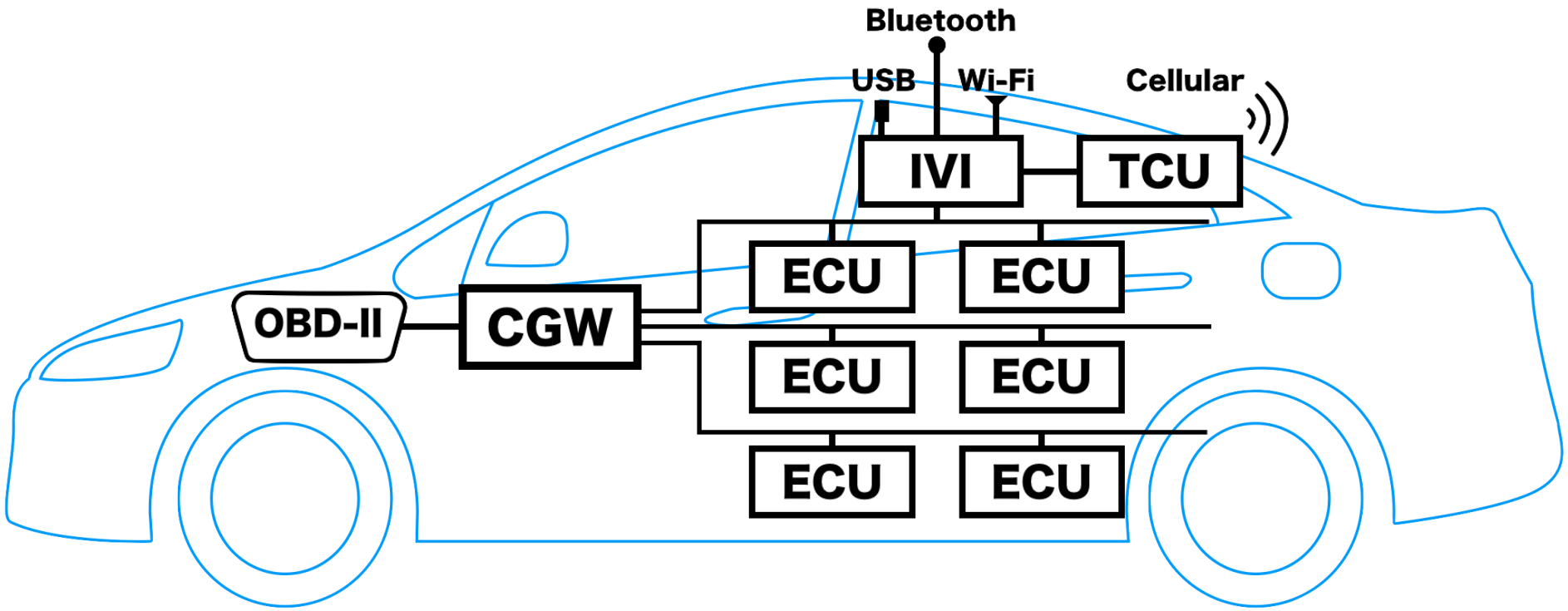
The median price here is $980,000

OPEC pump oil in three y

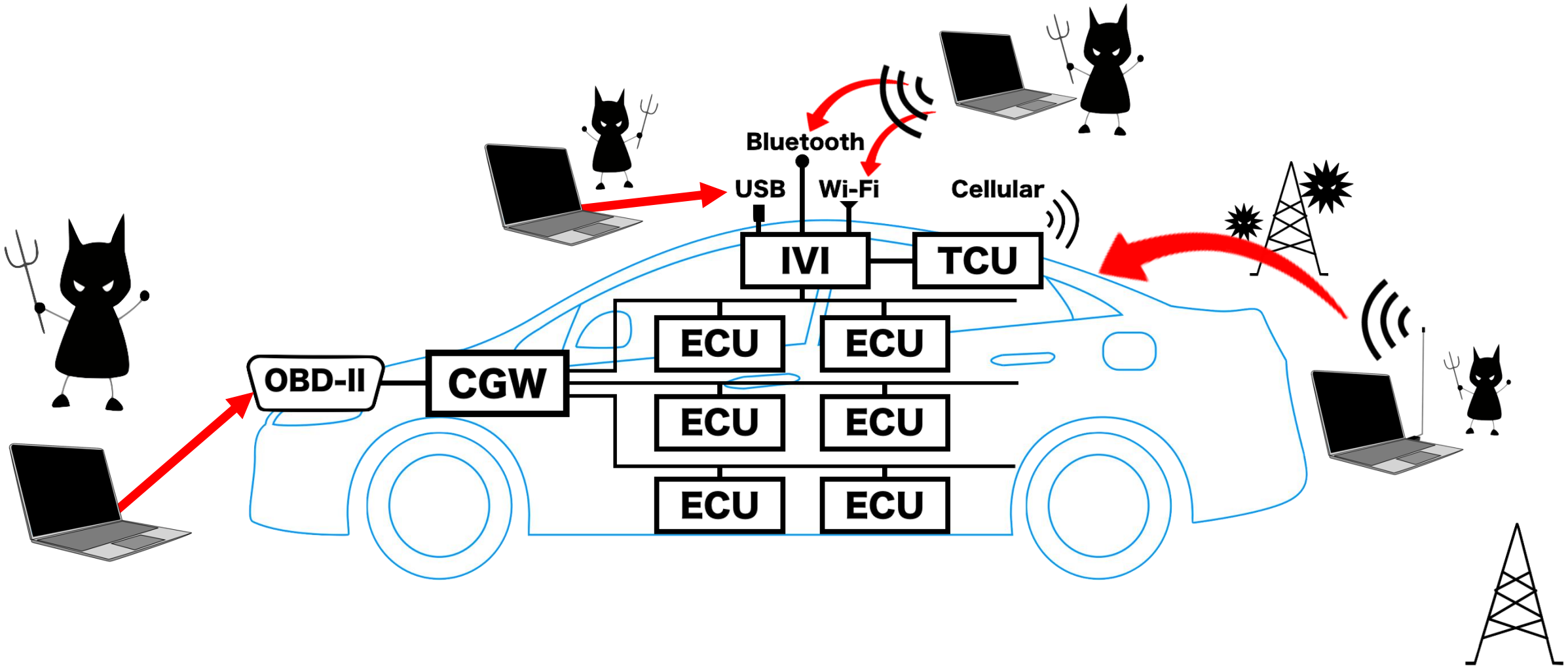
Problems in automotive industry

- Problems of cyber security technology for automobiles;
  - Delay in development of cyber security technology in automotive industry.
  - Lack of cyber security engineers in the automotive industry.

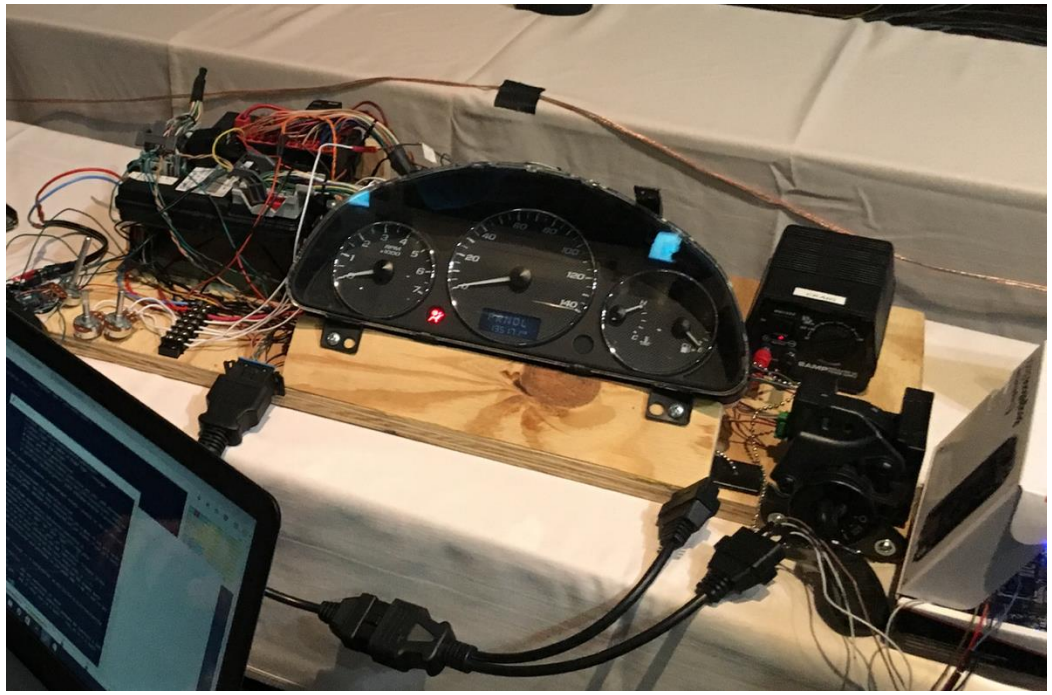
Typical architecture of a vehicle



Typical attack surfaces in recent vehicles



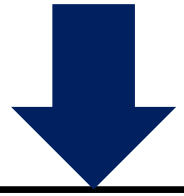
CAR HACKING VILLAGE in DefCon



Hacking event such as CTF is very fun! However, it is doubtful that it can be systematic way of learning vehicular security.

Motivation for developing platform

- There are no harmless real car for testers and no “generalized” one.
- We need to develop a platform not only for “Crack” but also “Hack”
  - Anyone can hack and study by “playground vehicle”
  - A newly proposed security technology can be evaluated its feasibility in common platform.



Open, safe, and attractive platform for vehicular cyber security is required

Philosophy of PASTA

Philosophy of PASTA

Open **Safe**

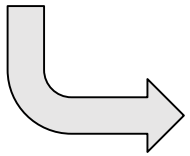
Adaptable **Portable**

Philosophy of PASTA

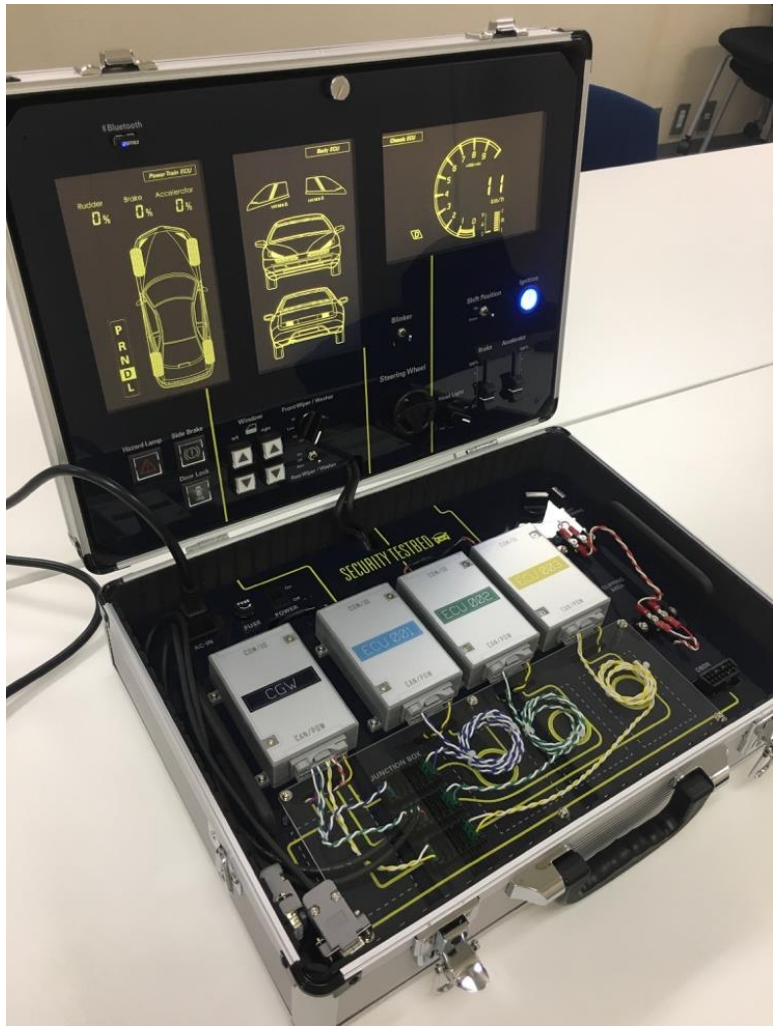
- **Open**
  - It must be based on non-proprietary technologies.
- **Adaptable**
  - Users should be able to rewrite the firmware of ECUs, re-design the architecture and connect their own devices, for example.
- **Safe**
  - There should be no real actuators; it can avoid incidents.
  - Such as wheels, brakes and window should be realized by simulator rather than the real things.
- **Portable**
  - Platform is preferred to be small and portable so that users can study, research, and hack it anywhere.

PASTA

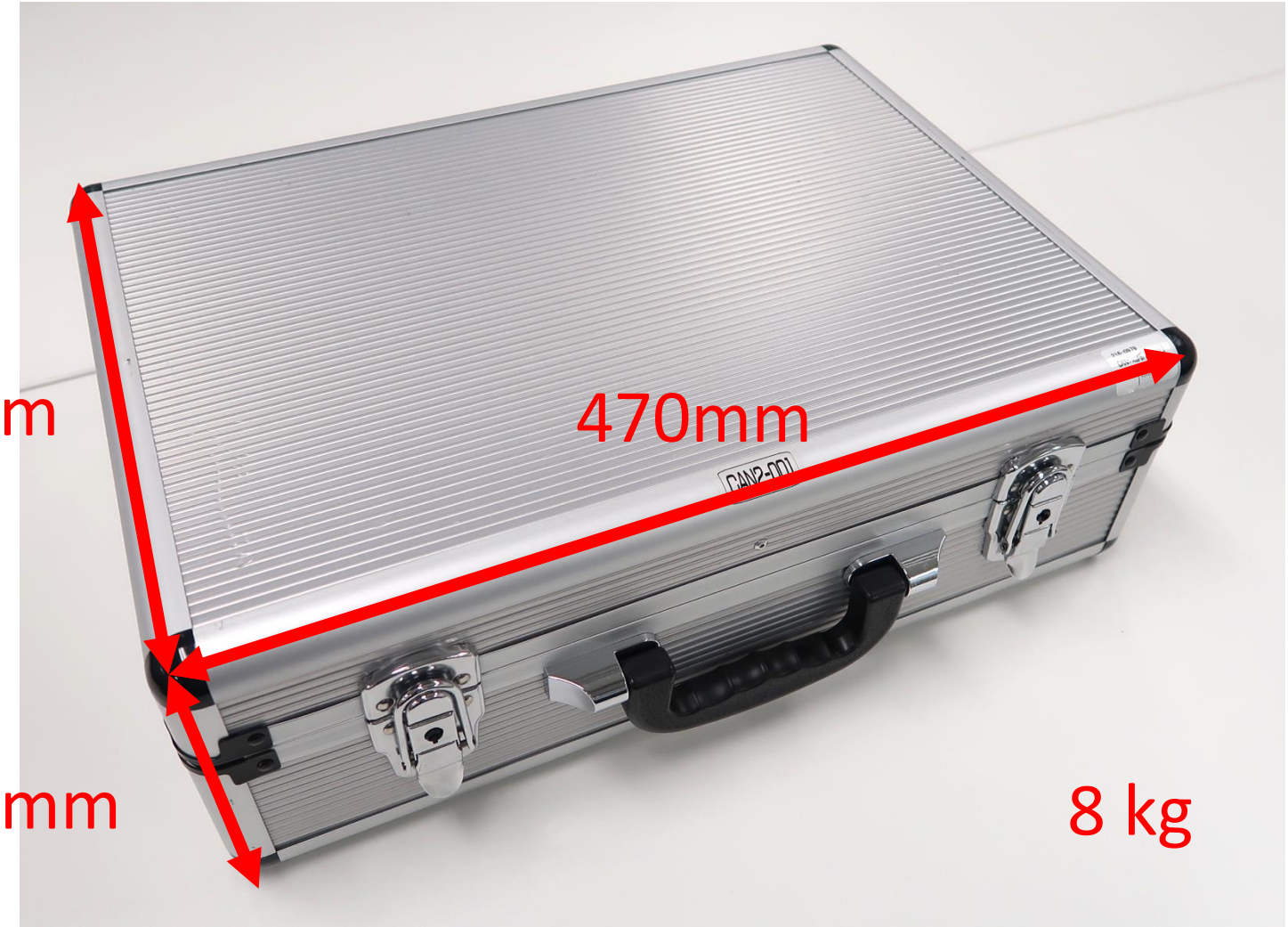
It seems an ordinary attaché case…



Once it opened,
PASTA appears.

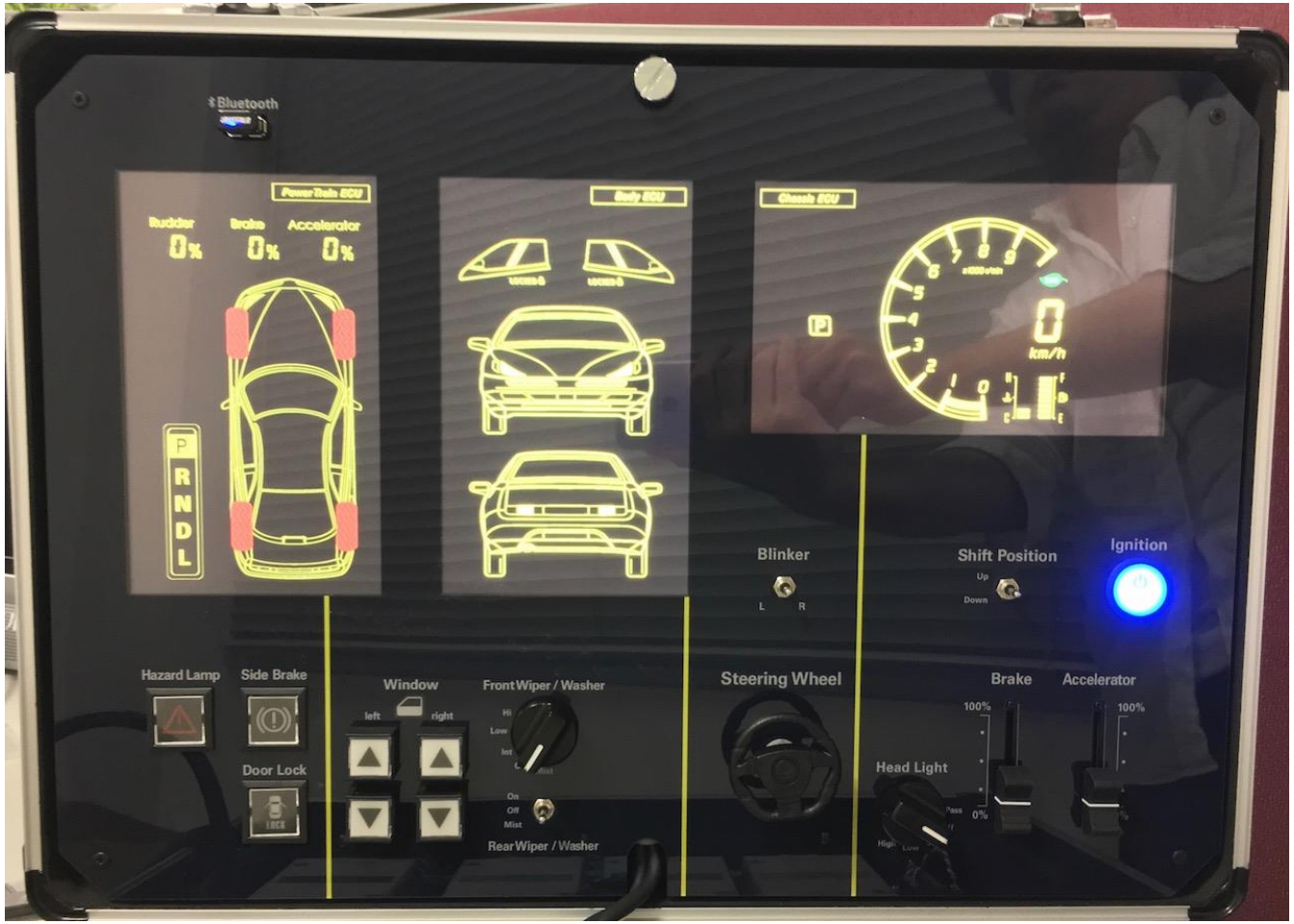


Portability of PASTA



Portable!

Upper side of PASTA



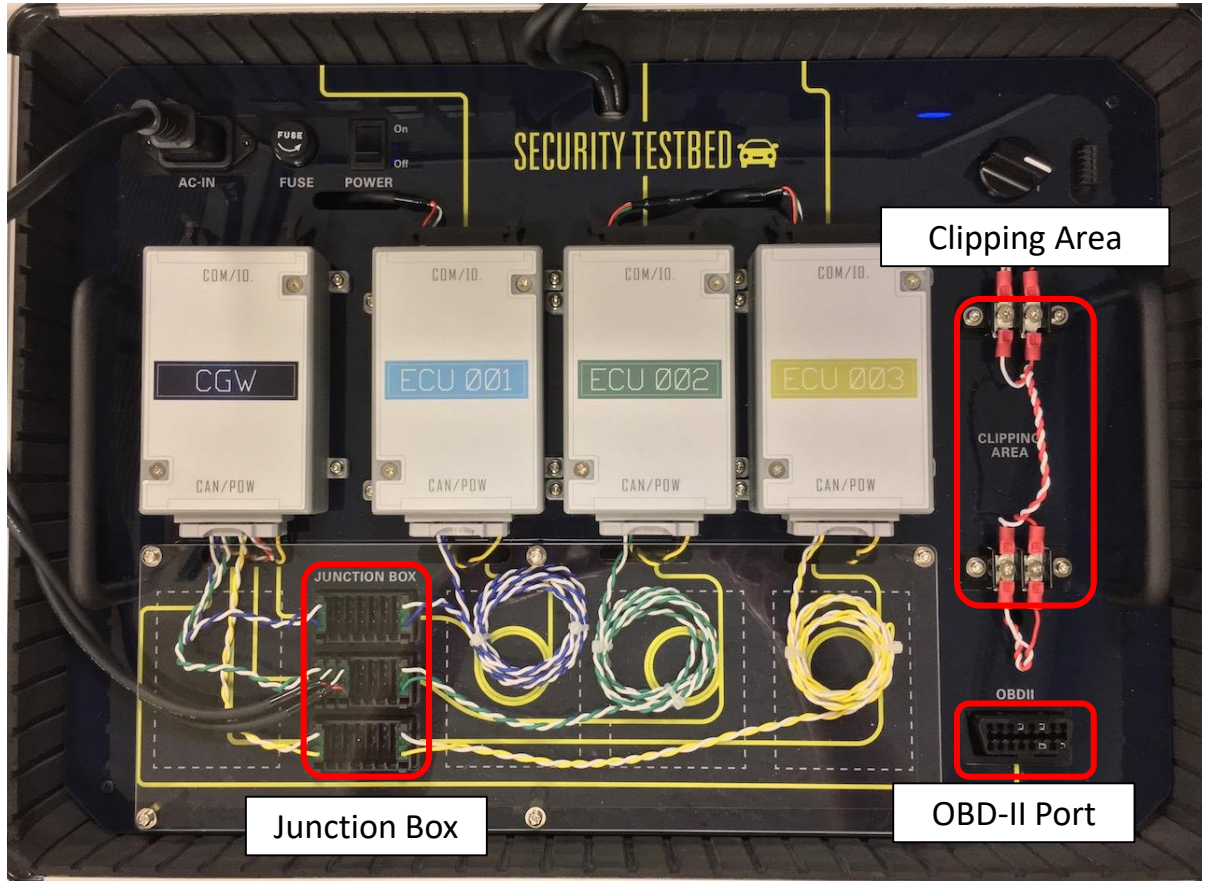
- There is a simple simulator in the attaché case, and it can be operated with the physical controller.
- The behavior by the operation can be confirmed from three LED panels.

SAFE!

Bottom side of PASTA

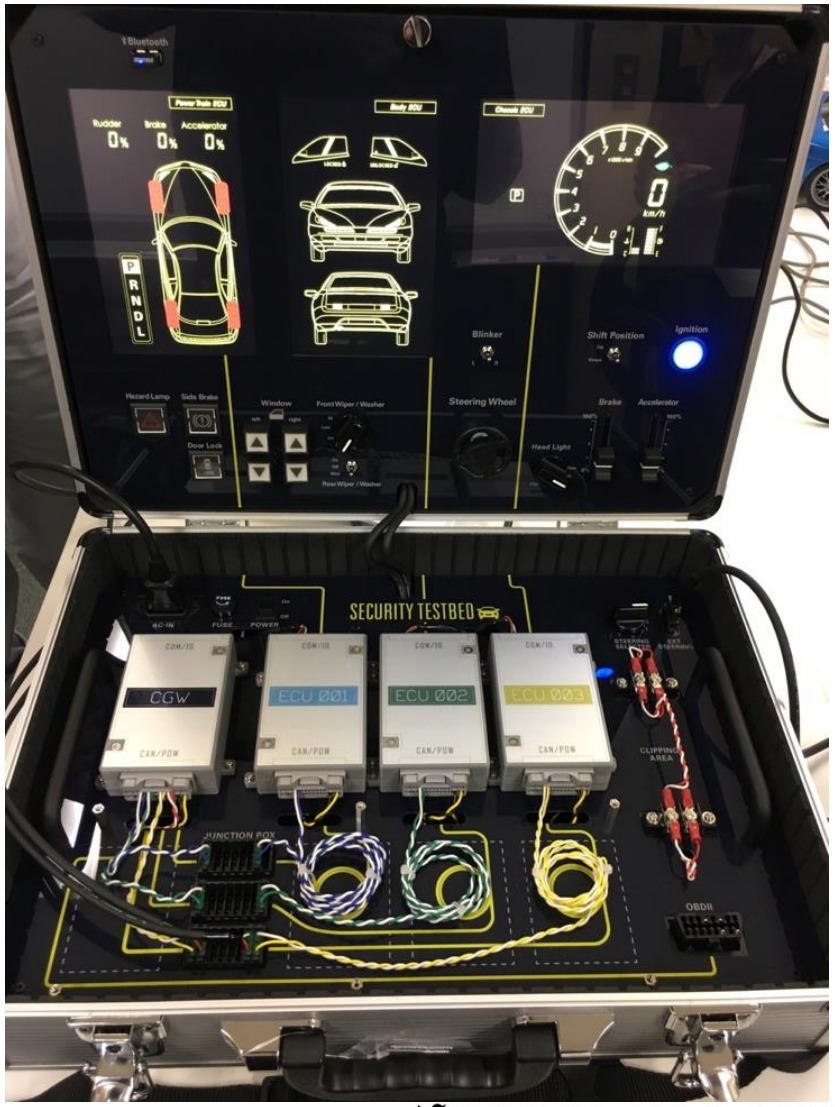
- Frequently used attack surfaces are equipped.
  - Since if it is easy to simulate a CAN message injection, security evaluation is easy.
- You can modify the program of these ECUs in C language.

Attack surfaces in PASTA

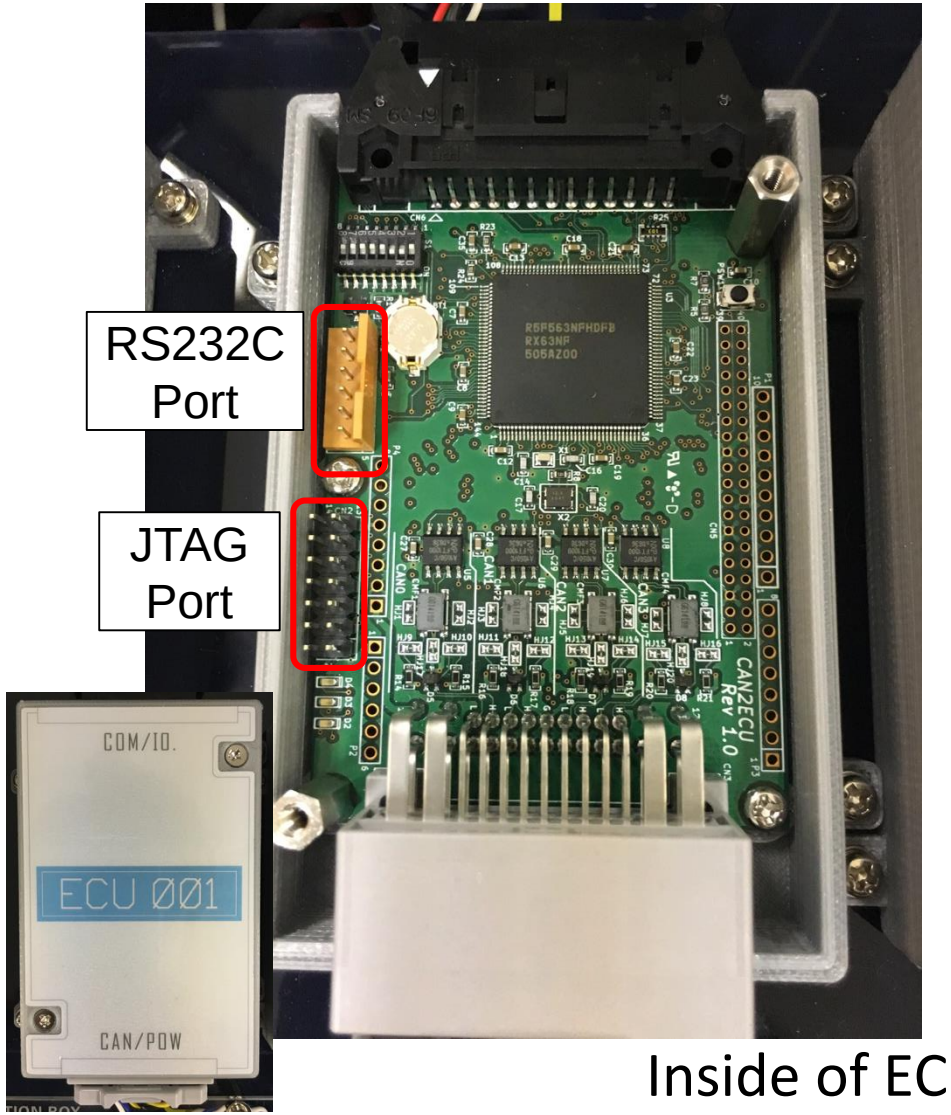


- Attack Surface are
  - OBD-II
  - Clipping Area
  - Junction Box
- Junction Box is implemented also for adaptability

Whole image of PASTA



Inside of the ECU

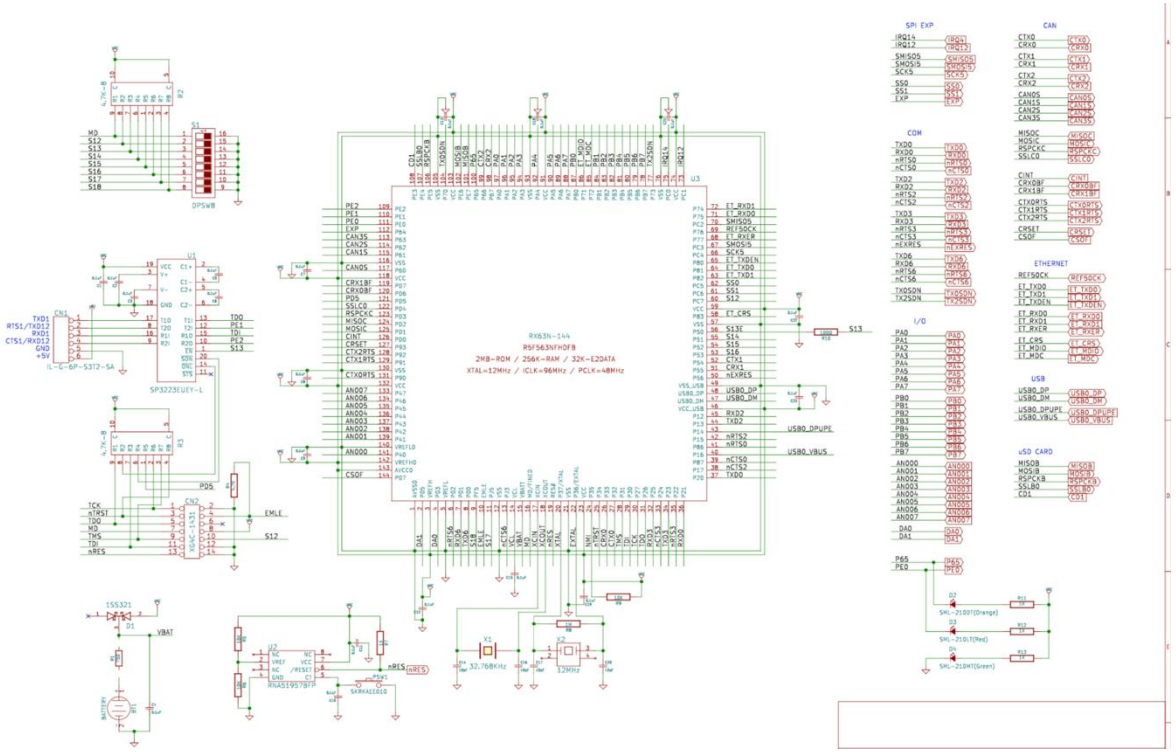


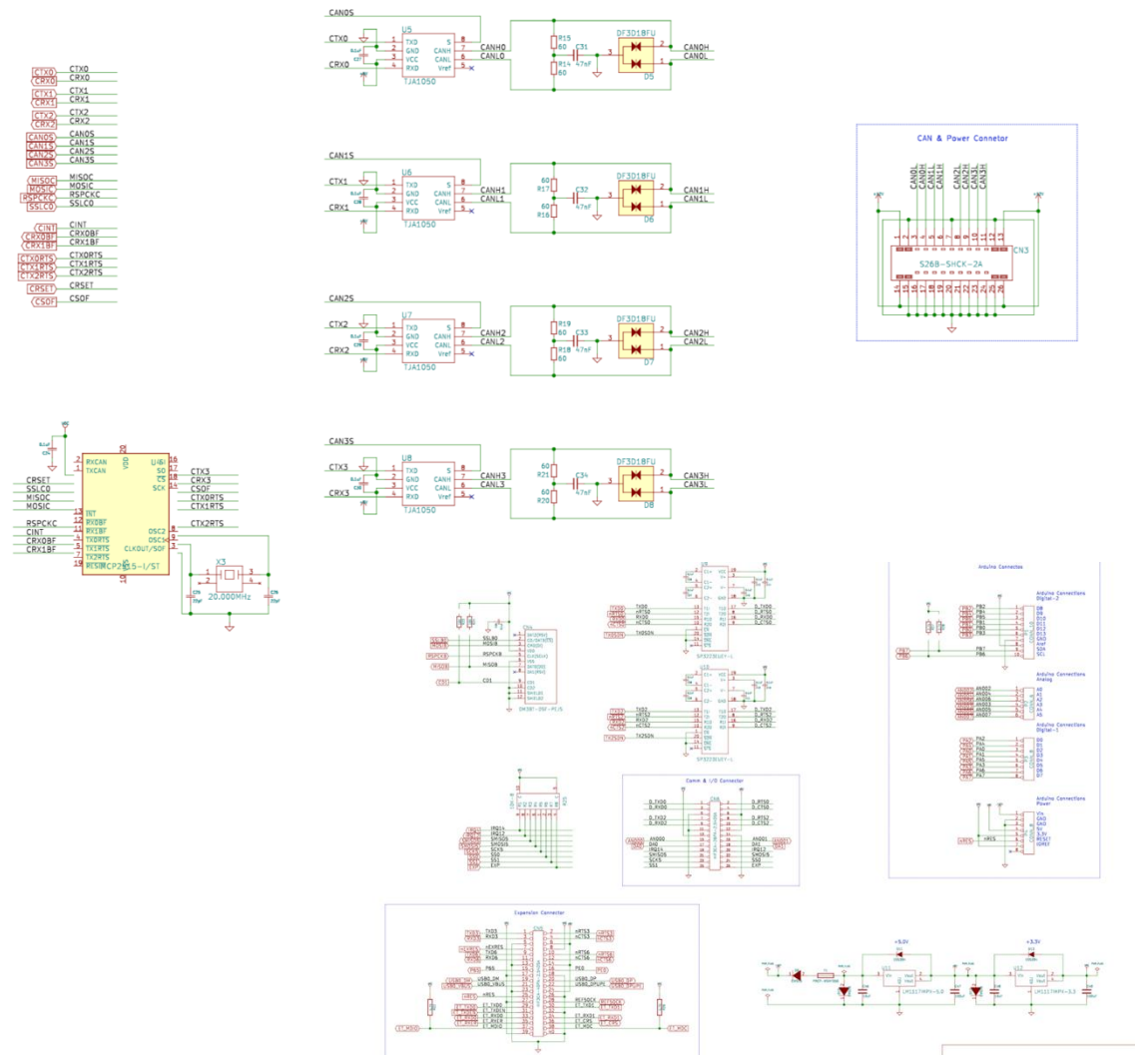
Inside of ECU

- Based on microcontroller(RX63N) by Renesas, we have designed and developed a ECU for PASTA from scratch.
- If you prepare for develop environment of Renesas microcontroller, you can apply your own program in C language.

Adaptable!

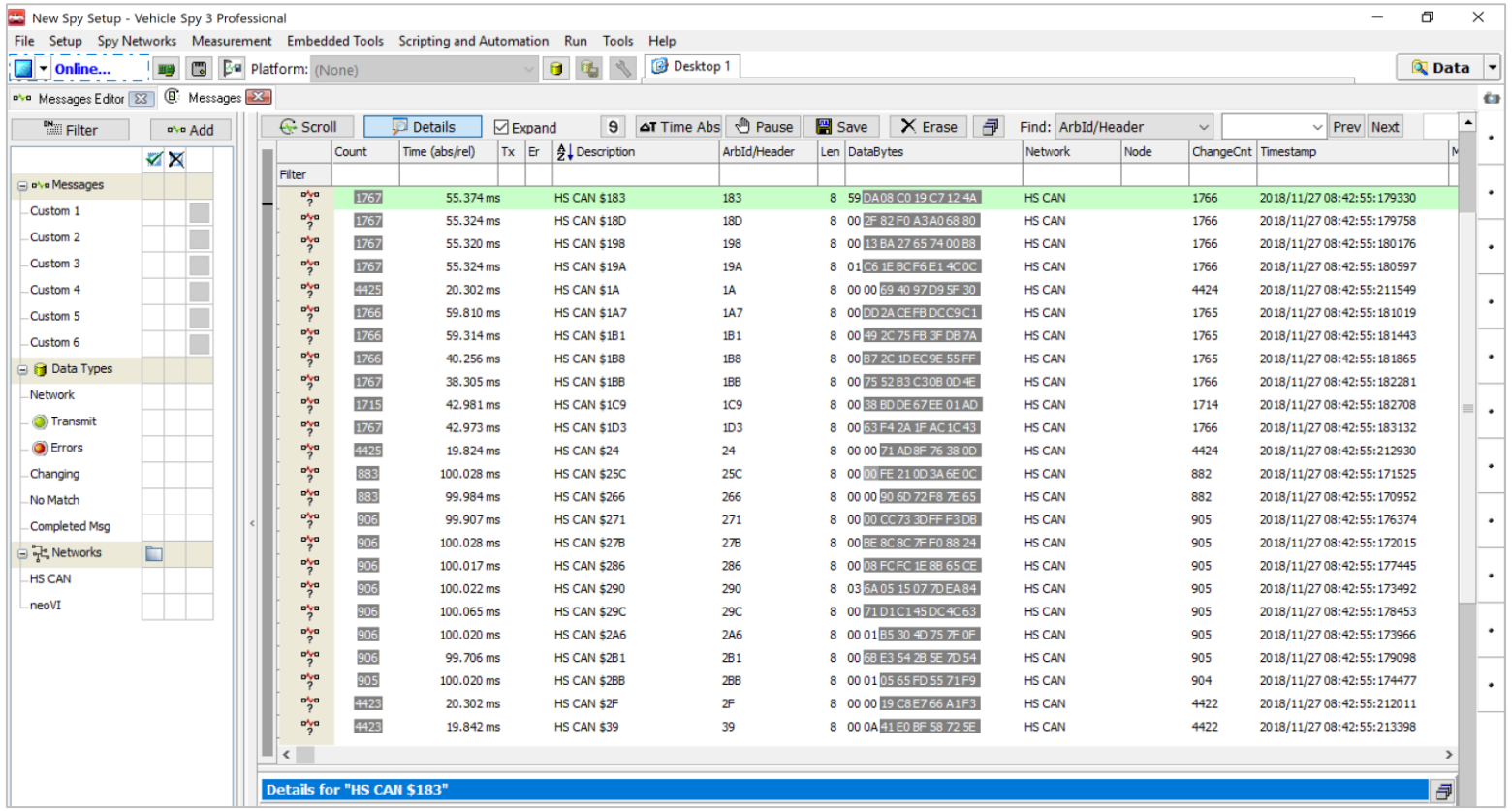
Design of the ECU





OPEN !

CAN IDs can be opened

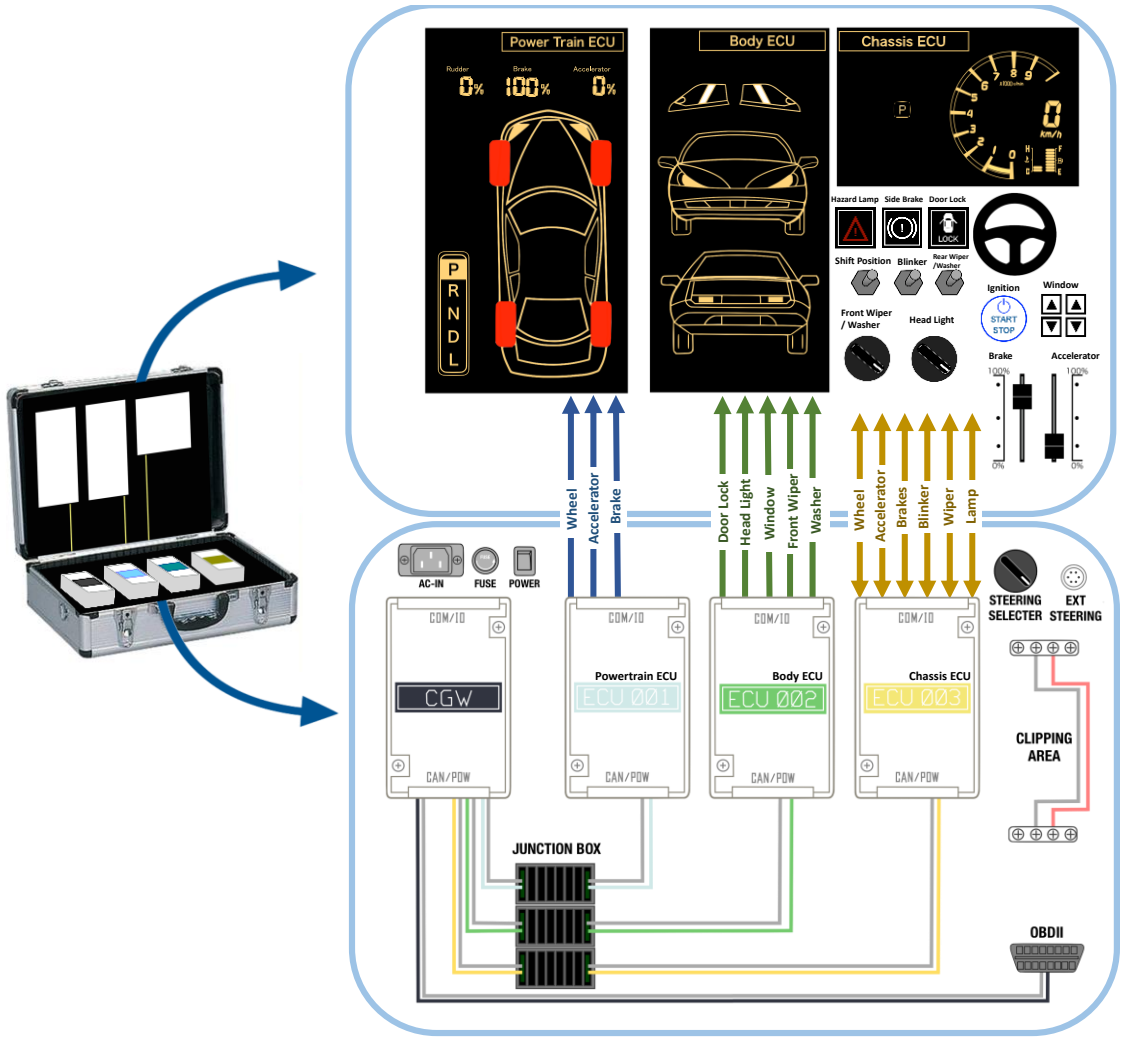


- 0x01A: Brake
- 0x02F: accelerator
- 0x1B1: headlight flashing
- 0x1B8: Ignition switch
- …

OPEN !

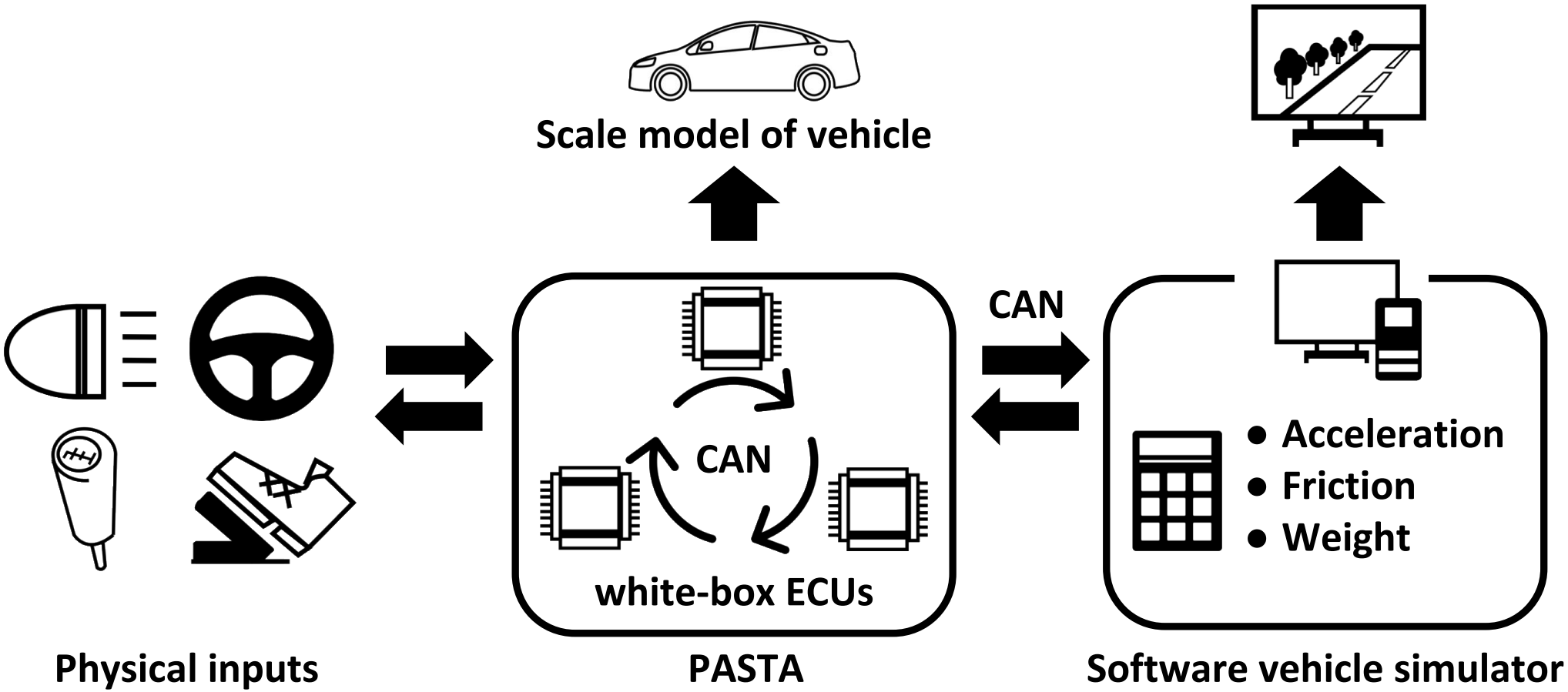
- CAN ID assignment table of PASTA is designed only for PASTA; Different from real vehicles.
- Users can create their own table and reprogram ECUs.

Information flow in PASTA



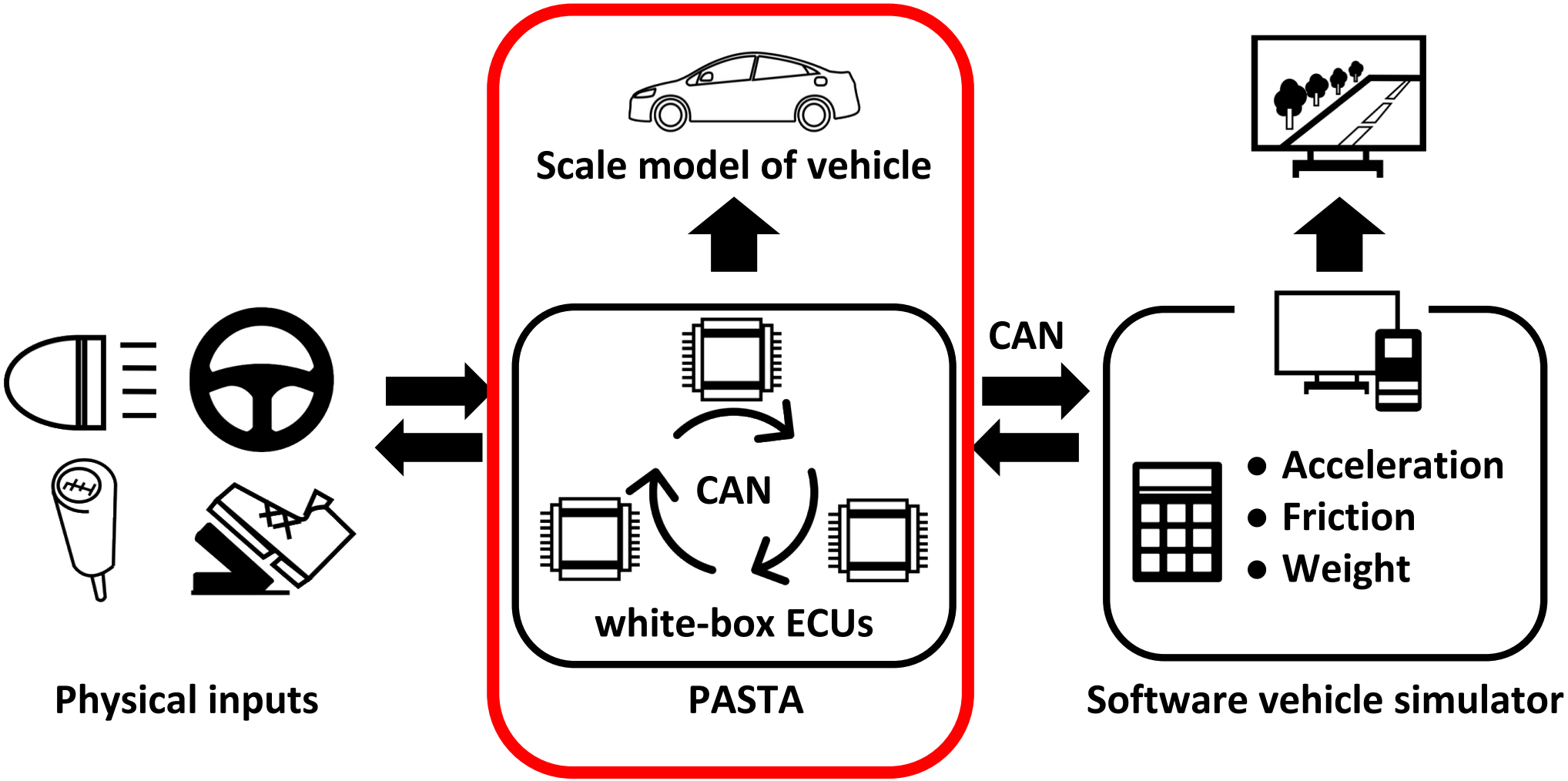
- In the attaché case, controller and vehicle simulator and ECUs are integrated.
- ECUs receive operations from controller, and ECUs send CAN messages. Thus ECUs share the information from operations and status of the vehicle.
- ECUs control actuators of simulator according to received CAN messages.

PASTA is adaptable



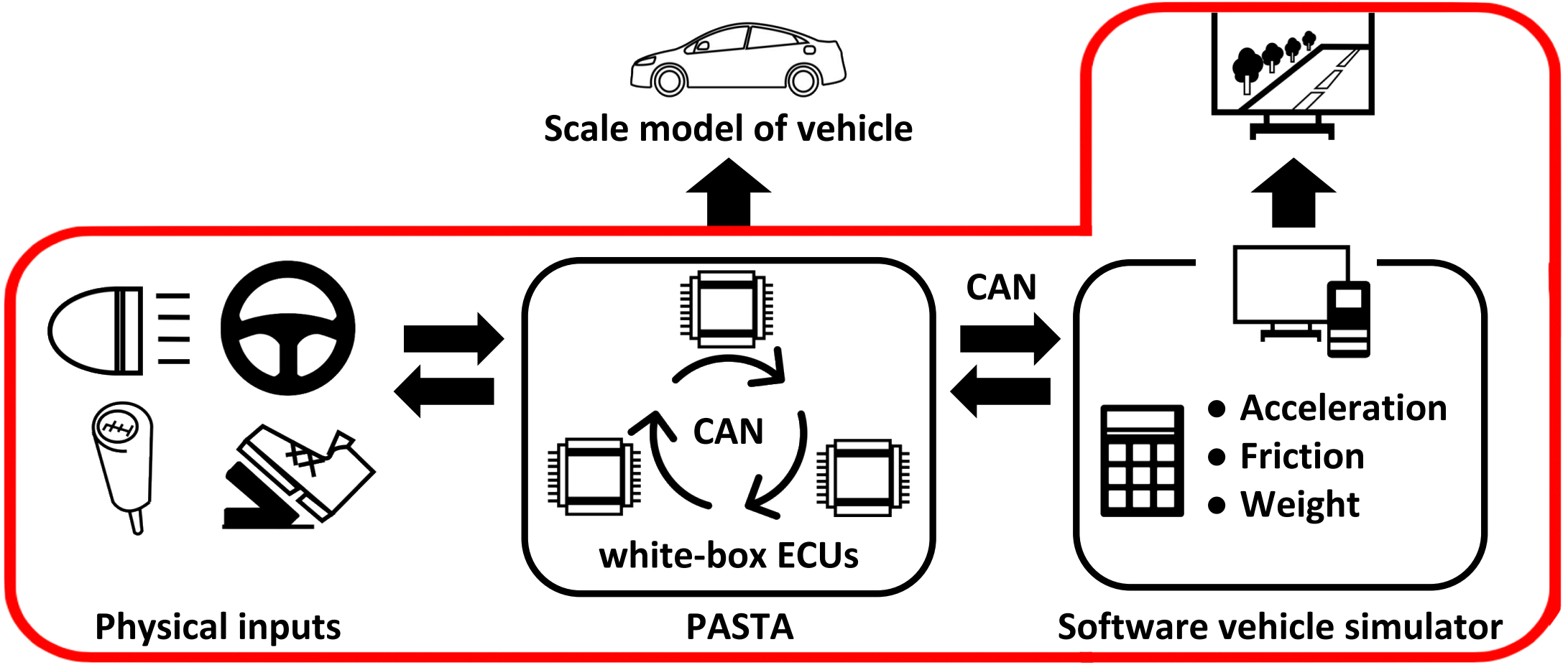
Demo

Demo of adaptability 1

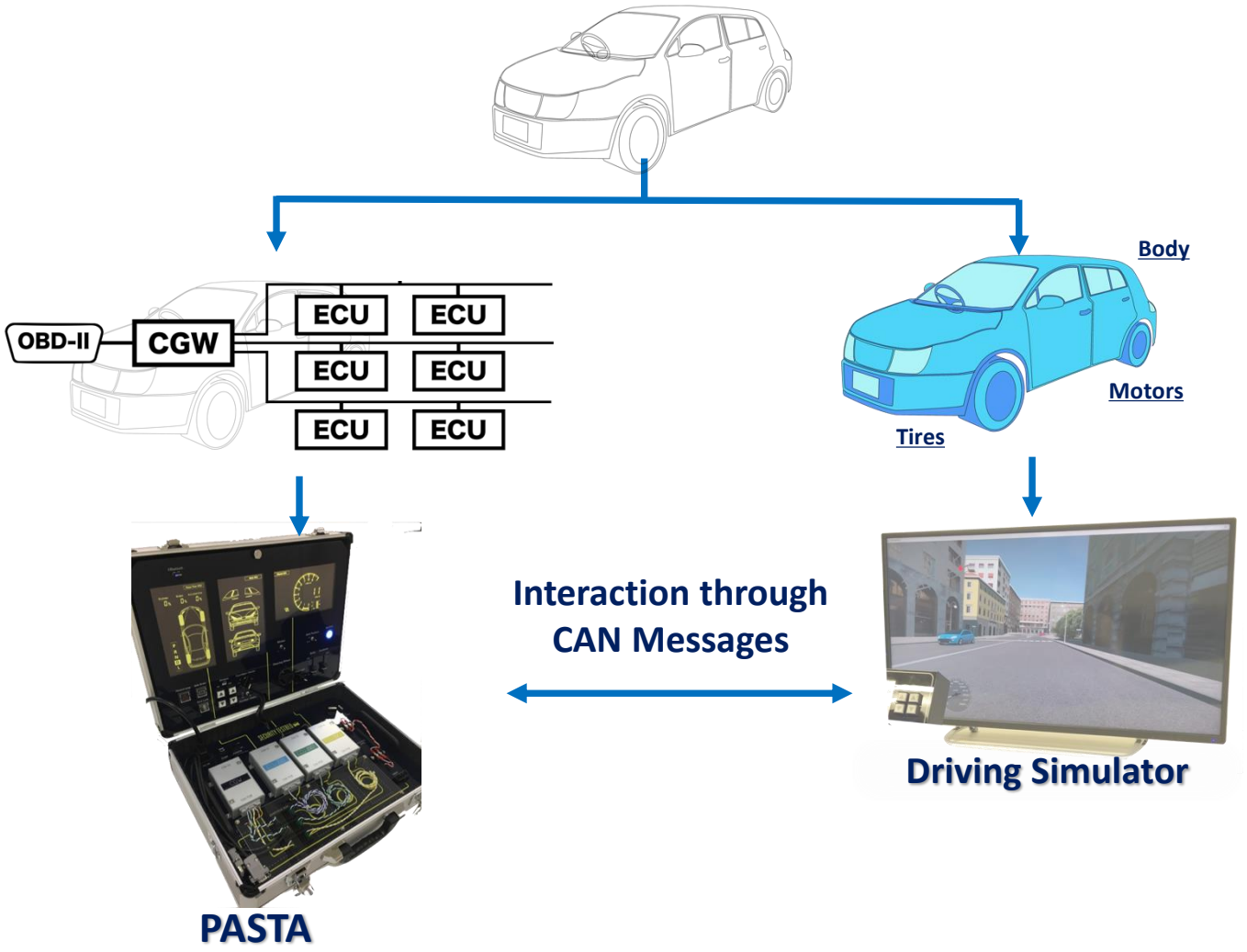


PASTSA with miniature vehicle

Demo of adaptability 2



Integration of drive simulator with PASTA

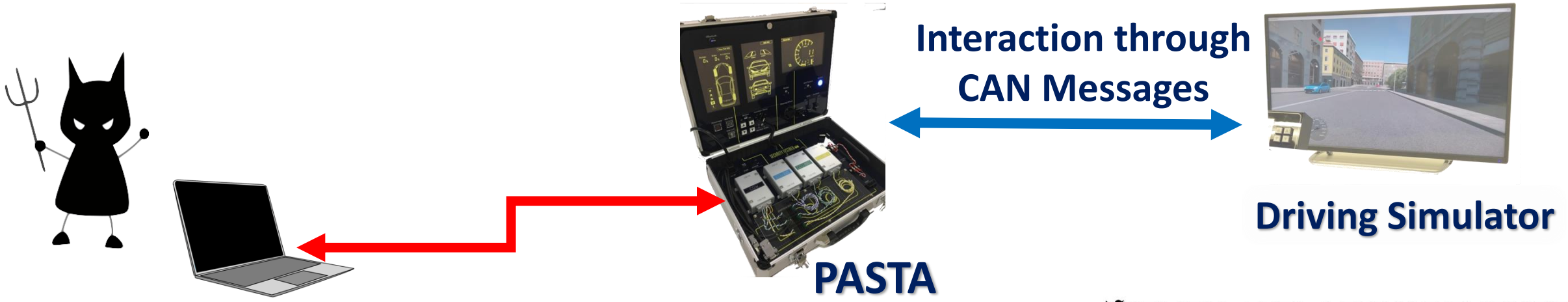


Real behavior by connection with a drive simulator

Demo: Incident…

Demo and CAUTION!!!

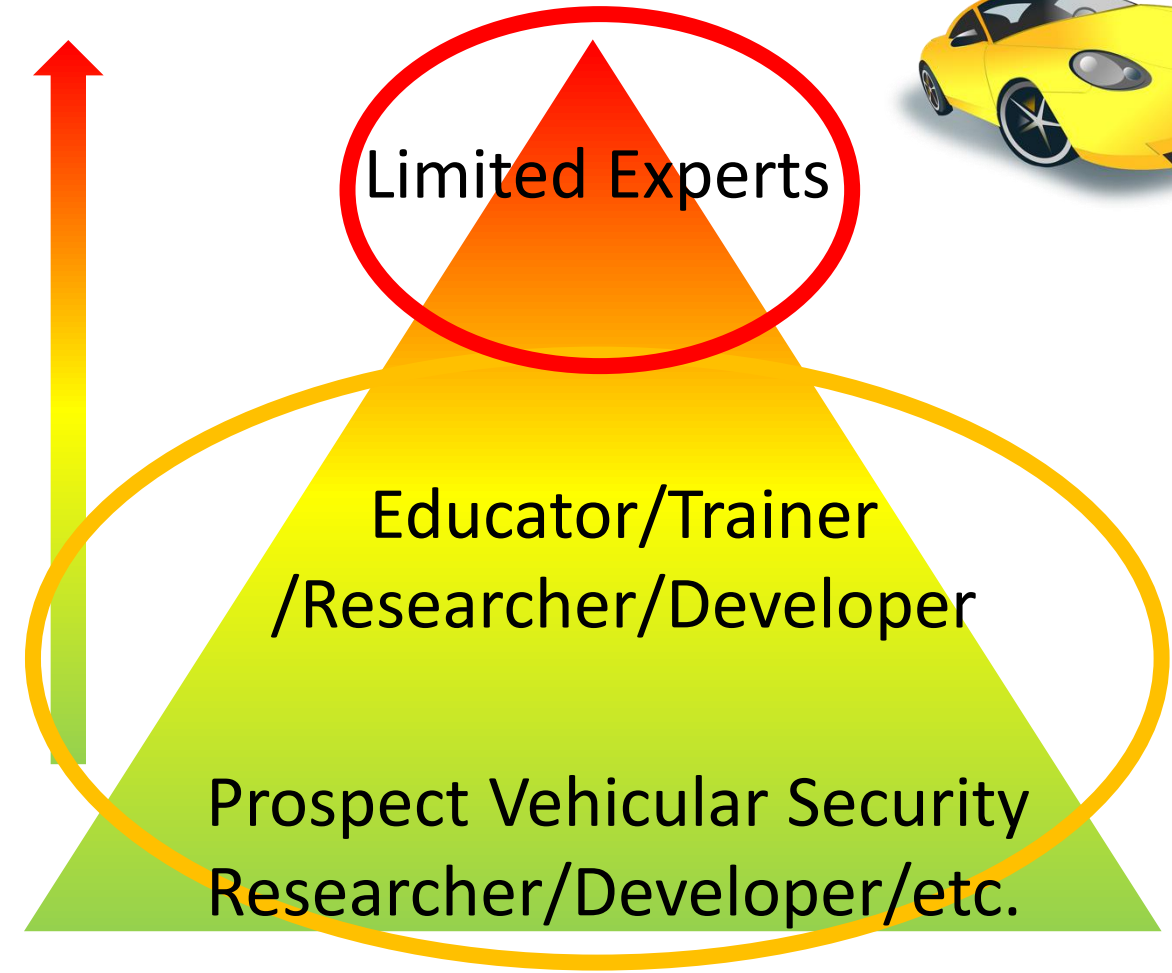
- Typical attack demonstration via OBD-II port: an attacker injects malicious CAN packets via OBD-II port.
- The effect of attack is noticeable, because, we have not implement enough safety function in software of ECUs in PASTA.
- However, real vehicles have security and safety functions, it is difficult to reproduce the result of following demo.



Demo: Incident…

Use Cases

Use Cases



Real Vehicle

WIRED

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

NOT for Everyone …

PASTA

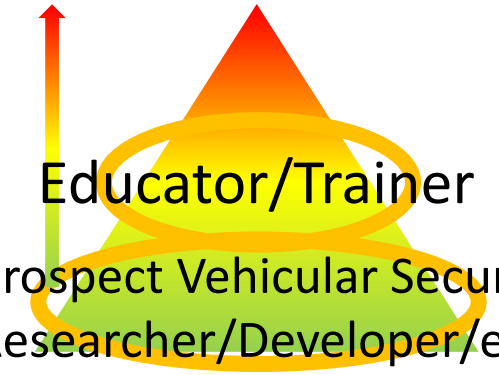
You can start if you have:
- Some space on desk
- An outlet

Open **Safe**

Adaptable **Portable**

Use Cases: Education/Training

TARGET



OBJECTIVE

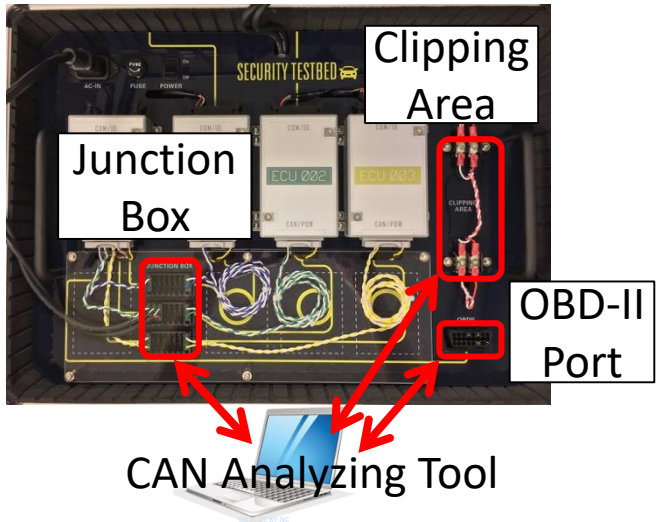
- Educate or learn vehicle security

REQUIRMENTS

- Open (e.g. known answers)
- Flexibility (e.g. intentionally embed vulnerabilities)
- Typical architecture
- Typical attack surfaces

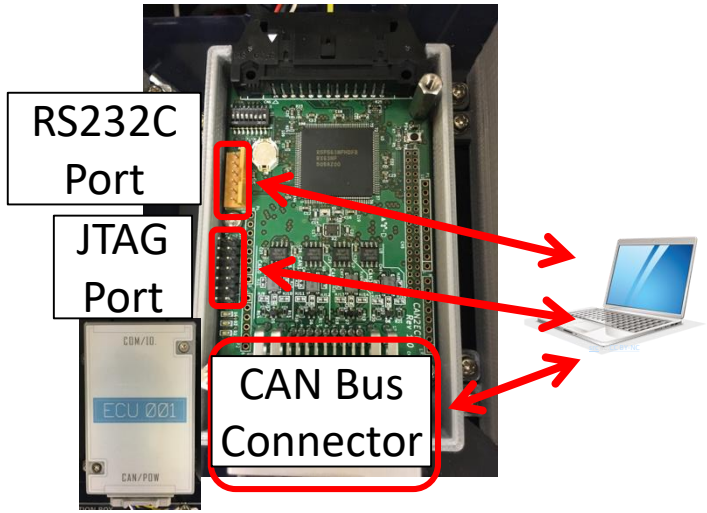
EXAMPLES

Hacking CAN bus messages



- Wire-tap, analyze, and inject CAN messages

Hacking ECU/CGW



- Read, analyze, and reprogram firmware

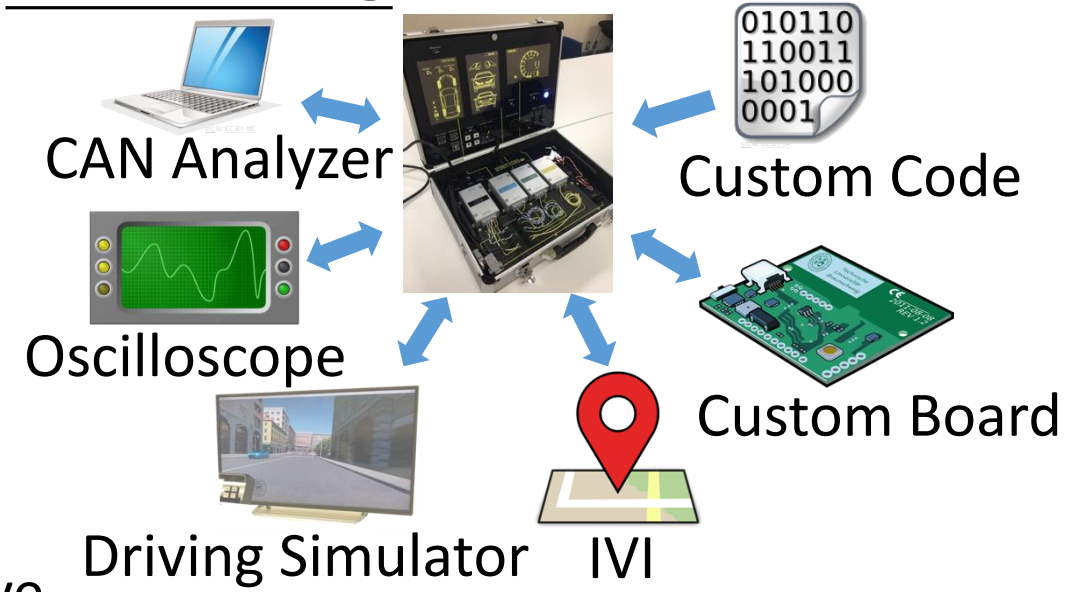
NOTES

- More to come:
  - LIN, CAN FD, IVI, Wireless I/F, etc.
- Joint work with YNU

Use Cases: Research

TARGET

EXAMPLES



OBJECTIVE

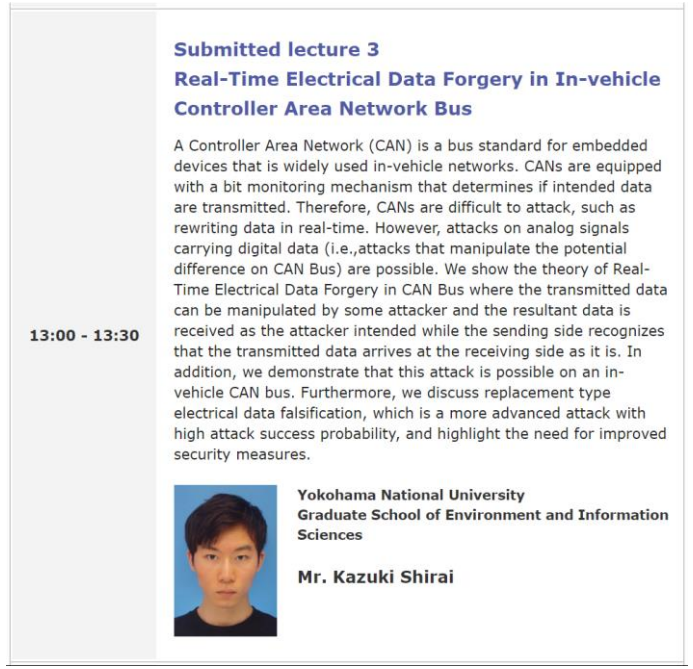
- Open research from various perspective

REQUIRMENTS

- Open
  - Publish the results
  - Reproduce environments and results

RESULTS

- **"Real-time Electrical Data Forgery in In-vehicle Controller Area Network Bus"** @ escar Asia 2018
  by K. Shirai, T. Kiyokawa, J. Sakamoto, T. Toyama, T. Matsumoto
  https://tech.nikkeibp.co.jp/cp/2018/escar2018e/



13:00 - 13:30

Submitted lecture 3

Real-Time Electrical Data Forgery in In-vehicle Controller Area Network Bus

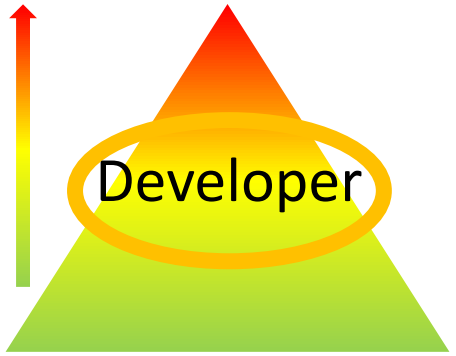
A Controller Area Network (CAN) is a bus standard for embedded devices that is widely used in-vehicle networks. CANs are equipped with a bit monitoring mechanism that determines if intended data are transmitted. Therefore, CANs are difficult to attack, such as rewriting data in real-time. However, attacks on analog signals carrying digital data (i.e.,attacks that manipulate the potential difference on CAN Bus) are possible. We show the theory of Real-Time Electrical Data Forgery in CAN Bus where the transmitted data can be manipulated by some attacker and the resultant data is received as the attacker intended while the sending side recognizes that the transmitted data arrives at the receiving side as it is. In addition, we demonstrate that this attack is possible on an in-vehicle CAN bus. Furthermore, we discuss replacement type electrical data falsification, which is a more advanced attack with high attack success probability, and highlight the need for improved security measures.

Yokohama National University
Graduate School of Environment and Information Sciences

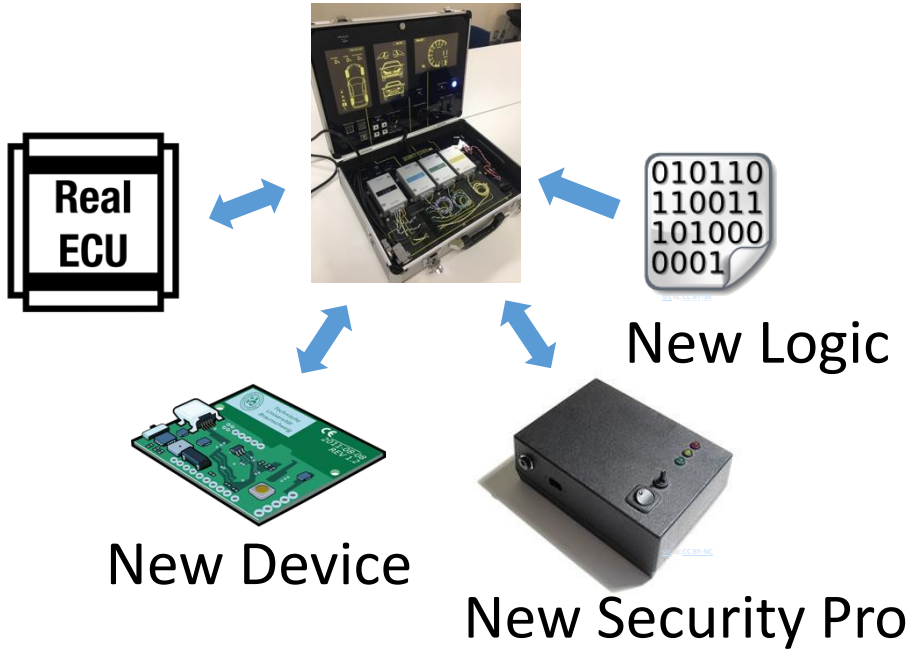
Mr. Kazuki Shirai

Use Cases: Development

TARGET



EXAMPLES



OBJECTIVE

- Prototyping and PoC of new technologies and products

REQUIRMENTS

- Simulates real vehicle
- Verify the effect
- Support various devices
- Adaptability

NOTES

- Require real vehicle in final process
- PASTA can be used for evaluation or validation of technologies and products

Roadmap

- For more advanced and realistic architecture:
  - Support **more protocols**
    - LIN, CAN FD, Ethernet, etc.
  - Support **wireless** interfaces
    - Wi-Fi, Bluetooth, Cellular
  - **IVI**
  - **More domains**
    - In-Vehicle Network of vehicles currently available are more complicated and have more domains.
  - Support **AUTOSAR** system
    - The ECUs in PASTA do not support any OS for vehicles and AUTOSAR system.
- **OPEN** specifications on GitHub

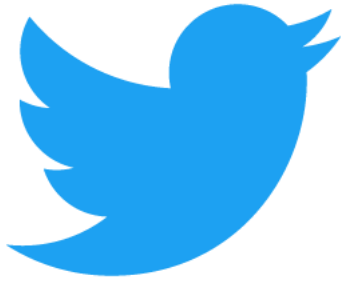
Take away

- In spite of vehicular security importance, any common platform for research has not been developed.

- PASTA is open, safe, adaptable and portable!
  - Apparently portable!
  - The design of PASTA is open; anyone can program and change the ECUs behavior.
  - PASTA is harmless for students, researchers, hackers, and so on because actuators are simulated in software.

- PASTA can be a common platform for…
  - Automotive cyber security research and development.
  - Educational tools.
  - etc…

For more information



@pasta_auto

GitHub https://github.com/pasta-auto

mail pasta_auto@jp.toyota-itc.com