PASTA: Portable Automotive Security Testbed with Adaptability

Tsuyoshi Toyama, Takuya Yoshida, Hisashi Oguma, Tsutomu Matsumoto
Who are we?

Tsuyoshi Toyama
Takuya Yoshida
Hisashi Oguma
Tsutomu Matsumoto
Agenda

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

- **OBD-II**: On-Board Diagnostics II interface
- **CGW**: Central Gateway
- **ECU**: Electronic Control Unit
- **IVI**: In-Vehicle Interface
- **TCU**: Telematics Control Unit
- **Bluetooth**, **USB**, **Wi-Fi**, **Cellular** connections
Typical attack surfaces in recent vehicles
Hacking event such as CTF is very fun! However, it is doubtful that it can be systematic way of learning vehicular security.
- 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**
  - It must be designed with adaptability so that users can connect their own devices or rewrite the firmware of ECUs, for example.

- **Safe**
  - By realizing actuators such as meter, steering wheel and brake with a simulator rather than the real things, it can avoid incidents for the user.

- **Portable**
  - Vehicles are so large that users cannot prepare the environment easily. Platform is preferred to be small and portable so that users can study, research, and hack it anywhere.
It seems an ordinary attaché case...

Once it opened, PASTA appears.
Portability of PASTA

Portable!

Dimensions:
- Length: 470 mm
- Width: 355 mm
- Height: 150 mm
- Weight: 8.3 kg
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 monitors.

SAFE!
- Frequently used attack surfaces are equipped.
- Since 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
Based on microcontroller (RX63N) by Renesas, we have designed and developed an ECU for PASTA from scratch.

If you prepare for develop environment of Renesas microcontroller, you can apply your own program in C language.

Programmable!
Design of the ECU

OPEN!
CAN IDs can be opened

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

OPEN!
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

Scale model of vehicle

Physical inputs

PASTA

white-box ECUs

Software vehicle simulator

- Acceleration
- Friction
- Weight

CAN

● Acceleration
● Friction
● Weight
Demo: normal
Demo of adaptability 1

Scale model of vehicle

Physical inputs

white-box ECUs

PASTA

CAN

ACCELERATION

FRICTION

WEIGHT

Software vehicle simulator

● Acceleration
● Friction
● Weight

Physical inputs

white-box ECUs

PASTA

CAN

Software vehicle simulator

● Acceleration
● Friction
● Weight

Physical inputs

white-box ECUs

PASTA

CAN

Software vehicle simulator

● Acceleration
● Friction
● Weight
PASTSA with miniature vehicle

(video – with miniature vehicle)
Demo of adaptability 2

Scale model of vehicle

Physical inputs

PASTA

white-box ECUs

CAN

Acceleration
Friction
Weight

Software vehicle simulator
Integration of drive simulator with PASTA

Interaction through CAN Messages
Real behavior by connection with a drive simulator

(video – 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 safety functions, it is difficult to reproduce the result of following demo.
(Video - incident)
Use Cases
Use Cases

Real Vehicle

Higher skills, more costs, advanced tools, equipment, ...

PASTA

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

Open Safe Adaptable Portable

NOT for Everyone ...
Use Cases: Education/Training

TARGET
Educator/Trainer
Prospect Vehicular Security Researcher/Developer/etc.

OBJECTIVE
• Educate or learn vehicle security

EXAMPLES
Hacking CAN bus messages
Junction Box
Clipping Area
OBD-II Port
CAN Analyzing Tool

• Wire-tap, analyze, and inject CAN messages

Hacking ECU/CGW
RS232C Port
JTAG Port
CAN Bus Connector

• Read, analyze, and reprogram firmware

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

NOTES
• More to come:
  • LIN, CAN FD, IVI, Wireless I/F support, etc.
  • On going or on roadmap
  • Joint work with YNU

OBJECTIVE
• Educate or learn vehicle security
Use Cases: Research

TARGET
Researcher

OBJECTIVE
• Open research from various perspective

REQUIREMENTS
• Publish the results
• Reproduce environments and results
• Physical/Logical, HW/SW, Analog/Digital
• Adaptability

EXAMPLES
- CAN Analyzer
- Oscilloscope
- Custom Code
- Custom Board
- Driving Simulator
- IVI

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/
Use Cases: Development

TARGET

Developer

OBJECTIVE

• Prototyping and PoC of new technologies and products

REQUIREMENTS

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

EXAMPLES

NOTES

• Require real vehicle in final process
• Can be used for evaluation 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.
  - Make specifications **OPEN** on GitHub
In spite of vehicular security importance, any common platform for research has not been developed.

PASTA is open, portable, safe, adaptable.
- 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.

The testbed 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