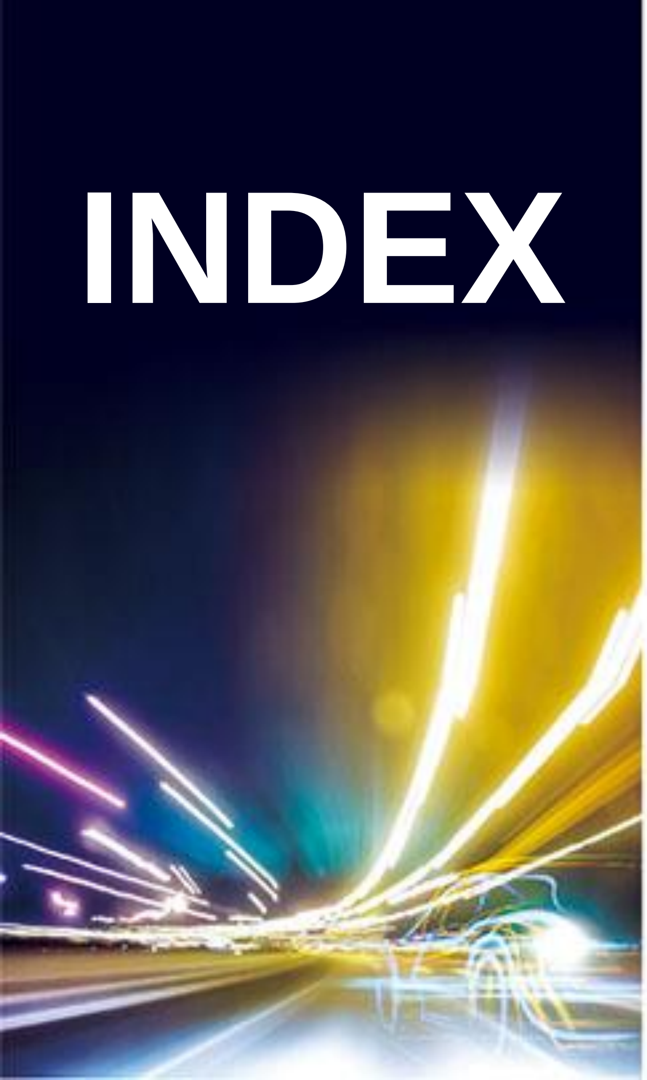
SIP-adus Workshop 2018

Current SIP-adus Activity for Vehicle-level Penetration Testing

Hiroshi Nodomi
PwC Consulting LLC

13th November 2018



INDEX

1. FOT* Project Overview
2. FOT Overall Schedule and FY2018 Schedule
3. Automated Driving System Threat Analysis
4. Information Security Evaluation Guideline
5. FY2018 Evaluation Criteria and Guideline Update

** FOT : Field Operational Test*

1. FOT Project Overview

◆ "Information Security" FOT is currently developing vehicle evaluation guideline that can be widely used by automotive manufacturers as well as suppliers.

Environment around Automated Driving System

- It is expected that **information used as the foundation for automated driving systems will be obtained from external networks**
  (e.g. high definition map data, data on vehicles, pedestrian, road infrastructure etc.)
- Using such information for vehicle control in the automated driving system could lead to **cause cybersecurity issues that did not exist in conventional cars**.

Purpose and Overview of "Information Security" Field Operational Test

Conduct research/analysis on security threat related to the automated driving, **develop security evaluation method/protocol (guideline) at vehicle/component level** towards international standardization, **conduct technical research to assess the cybersecurity endurance based on black-box testing** on actual vehicle systems provided by the participants of the FOT.

1. Establish evaluation method against attacks using vehicle communication
2. Formulate comprehensive threat model for external vehicular attacks such as V2X
3. Build consensus on cybersecurity of automated driving vehicles
4. Develop professional resources and accumulate know-how related to security of automated driving vehicles in Japan

2. FOT Overall Schedule and FY2018 Schedule

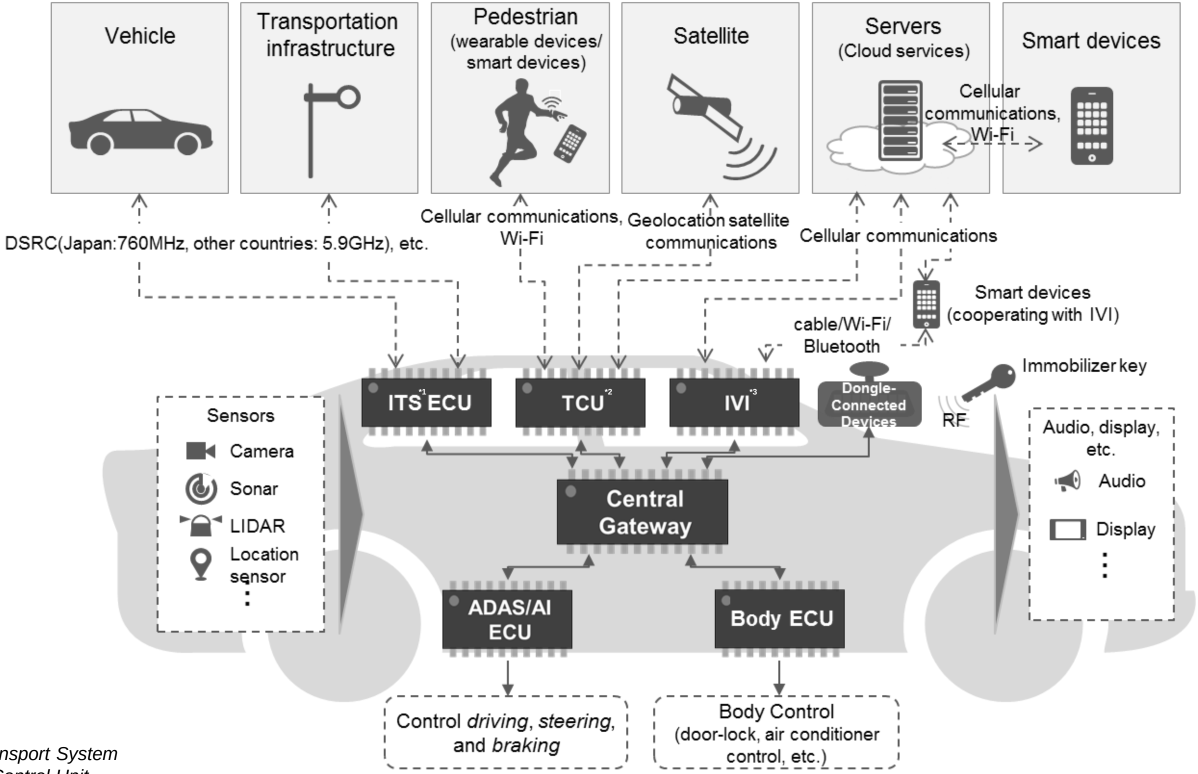
◆ In FY2018, black-box tests will be conducted on multiple vehicle systems based on the evaluation guideline(draft) developed in FY2017. Based on the results, the guideline will be updated to a final version.

Project Phase	Item	Details	Period
FY2017 Trial Research (Step 1)	Security Threat Analysis on Automated Driving System	• Research/analyze/clarify security threats for automated driving systems including vehicles and infrastructure.	2017/9 ~ 2018/2
	Develop Draft of Information Security Evaluation Guideline	• Develop initial draft of the guideline based on known incidents, vulnerabilities and security evaluation methods. • Conduct trial research on actual vehicle system based on the initial draft of the guideline. • Develop second draft of the guideline based on the result.	
	Conduct Trial Research on Information Security Evaluation		
FY2018 FOT (Step 2)	Prepare for FOT	• Recruit Japanese OEMs to participate in the FOT. • Coordinate vehicle systems to be provided for the FOT, evaluation environment/period etc. with the participants.	2018/4 ~ 2018/7
	Conduct Information Security Evaluation	• Conduct security evaluation based on the draft of the evaluation guideline developed in STEP1 against the vehicle systems provided by the FOT participants.	2018/8 ~ 2019/2
	Finalize Information Security Evaluation Guideline	• Finalize the evaluation guideline by reflecting the improvement points clarified through analysis of the evaluation results.	

3. Automated Driving System Threat Analysis

Common Model for Automated Driving System

* The topologies of control functions related to steering, brakes, engines, etc. were abstracted as they do not directly affect the security threat analysis results.



Vehicle

Transportation infrastructure

Pedestrian (wearable devices/ smart devices)

Satellite

Servers (Cloud services)

Smart devices

Cellular communications, Wi-Fi

DSRC(Japan:760MHz, other countries: 5.9GHz), etc.

Cellular communications, Wi-Fi

Geolocation satellite communications

Cellular communications

Smart devices (cooperating with IVI)

cable/Wi-Fi/ Bluetooth

Immobilizer key

RF

ITS ECU[*1]

TCU[*2]

IVI[*3]

Dongle-Connected Devices

Sensors

Camera

Sonar

LIDAR

Location sensor

⋮

Central Gateway

ADAS/AI ECU

Body ECU

Audio, display, etc.

Audio

Display

⋮

Control *driving*, *steering*, and *braking*

Body Control (door-lock, air conditioner control, etc.)

[*1] *ITS: Intelligent Transport System*

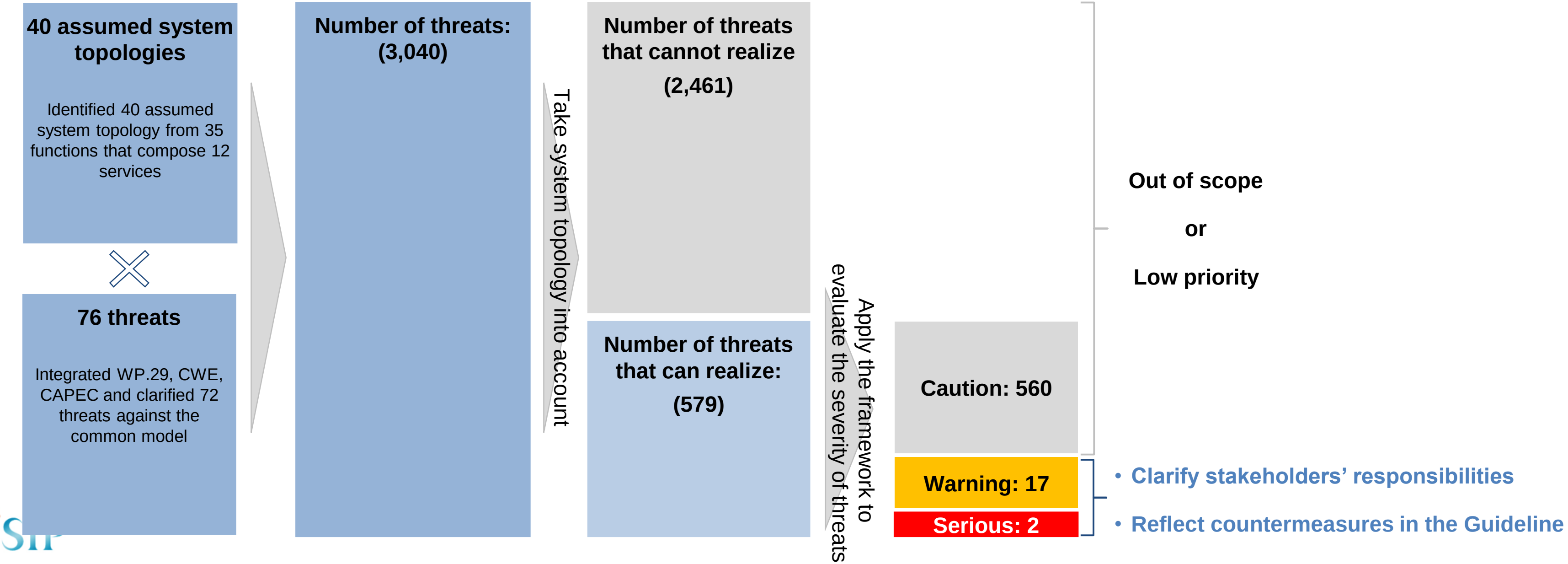
[*2] *TCU: Telematics Control Unit*

[*3] *IVI: In-Vehicle Infotainment System*

3. Automated Driving System Threat Analysis

Summary of Approach for Research on Threat

- Based on all the systems related to the common model, identify threats that can be realized, and clarify threats to be handled with priority by using the severity evaluation framework.
- Against the identified threats, clarify the responsible stakeholders of countermeasures and reflect threats that need countermeasures in the evaluation guideline.



40 assumed system topologies

Identified 40 assumed system topology from 35 functions that compose 12 services

76 threats

Integrated WP.29, CWE, CAPEC and clarified 72 threats against the common model

Number of threats: (3,040)

Take system topology into account

Number of threats that cannot realize (2,461)

Number of threats that can realize: (579)

Apply the framework to evaluate the severity of threats

Caution: 560

Warning: 17

Serious: 2

Out of scope

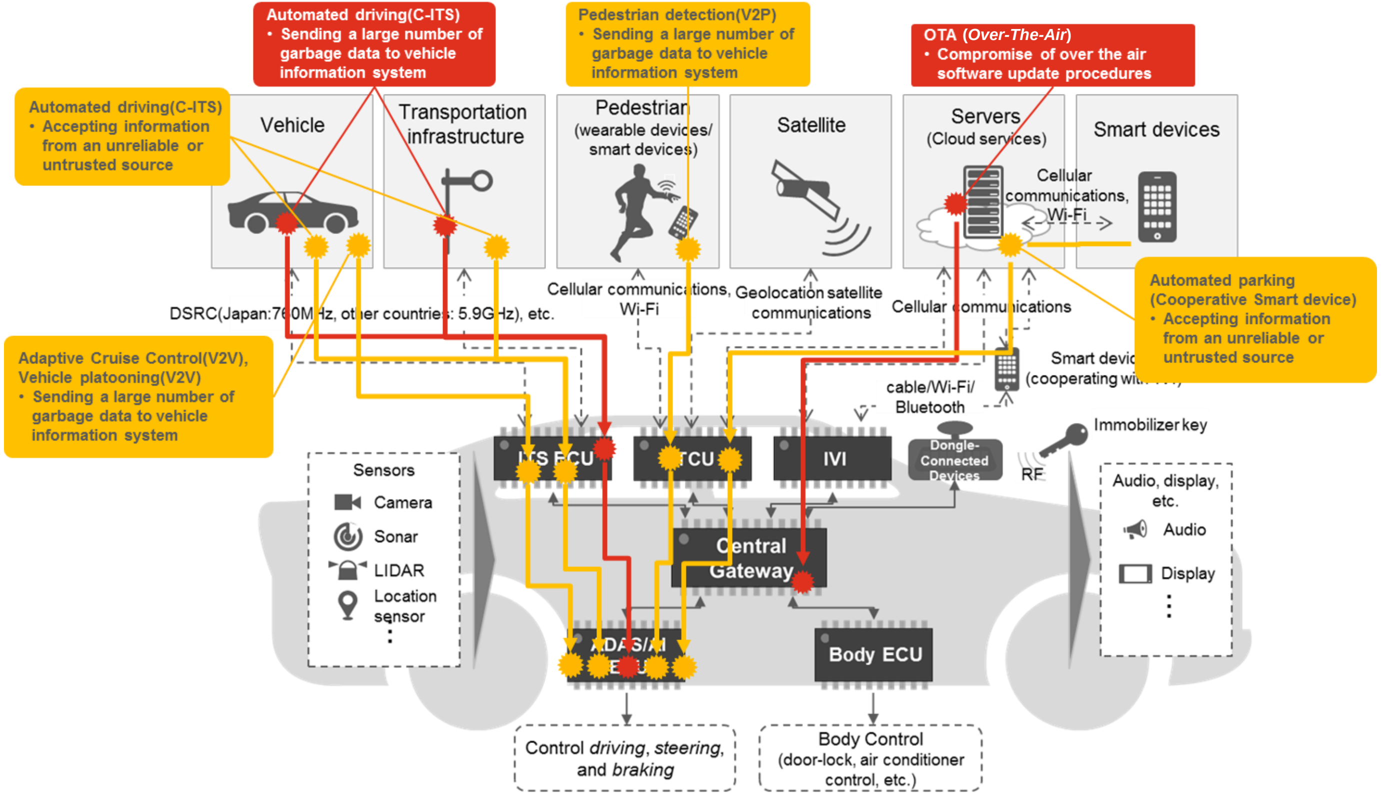
or

Low priority

- **Clarify stakeholders' responsibilities**
- **Reflect countermeasures in the Guideline**

3. Automated Driving System Threat Analysis

Whole picture of threat for the common model



Automated driving(C-ITS)
- Sending a large number of garbage data to vehicle information system

Pedestrian detection(V2P)
- Sending a large number of garbage data to vehicle information system

OTA (*Over-The-Air*)
- Compromise of over the air software update procedures

Automated driving(C-ITS)
- Accepting information from an unreliable or untrusted source

Adaptive Cruise Control(V2V), Vehicle platooning(V2V)
- Sending a large number of garbage data to vehicle information system

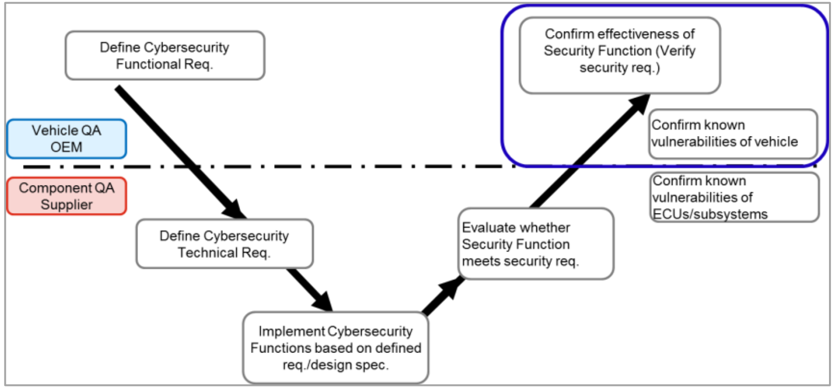
Automated parking (Cooperative Smart device)
- Accepting information from an unreliable or untrusted source

Vehicle
Transportation infrastructure
Pedestrian (wearable devices/ smart devices)
Satellite
Servers (Cloud services)
Smart devices
Cellular communications, Wi-Fi
DSRC(Japan:760MHz, other countries: 5.9GHz), etc.
Cellular communications, Wi-Fi
Geolocation satellite communications
Cellular communications
Smart device (cooperating with IVI)
cable/Wi-Fi/ Bluetooth
Immobilizer key
Dongle-Connected Devices
RF
ITS ECU
TCU
IVI
Central Gateway
ADAS/AD ECU
Body ECU
Sensors
Camera
Sonar
LIDAR
Location sensor
⋮
Audio, display, etc.
Audio
Display
⋮
Control *driving*, *steering*, and *braking*
Body Control (door-lock, air conditioner control, etc.)

4. Overview and scope of Evaluation Guideline

Scope

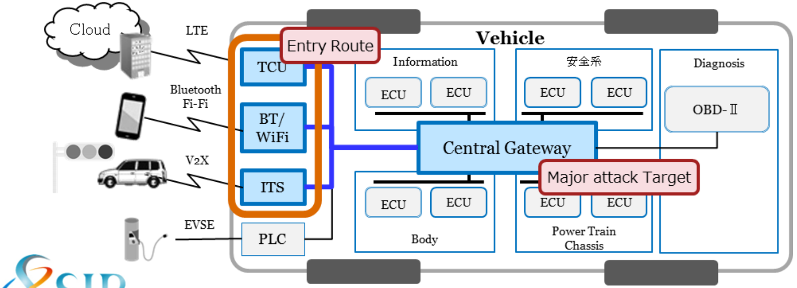
The guideline is developed towards contributing to comprehensive evaluation in V model of the vehicle development process, based on the results of discussion with stakeholders such as OEMs, etc.



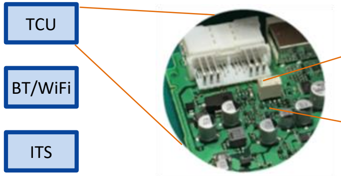
Vehicle QA
OEM
Component QA
Supplier
Define Cybersecurity Functional Req.
Define Cybersecurity Technical Req.
Implement Cybersecurity Functions based on defined req./design spec.
Evaluate whether Security Function meets security req.
Confirm effectiveness of Security Function (Verify security req.)
Confirm known vulnerabilities of vehicle
Confirm known vulnerabilities of ECUs/subsystems

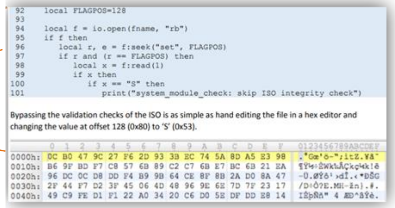
Characteristics of the Evaluation Method

1. Evaluation through intrusion testing from vehicle’s external interface from actual hacker(attacker)’s viewpoint



2. Evaluate hardware security functions taking into consideration actual attacks to the vehicles





```
local FLAGPOS=128

local f = io.open(fname, "rb")
if f then
   local r, e = f:seek("set", FLAGPOS)
   if r and (r == FLAGPOS) then
      local x = f:read(1)
      if x then
         if x == "S" then
            print("system_module_check: skip ISO integrity check")
```

Bypassing the validation checks of the ISO is as simple as hand editing the file in a hex editor and changing the value at offset 128 (0x80) to ‘S’ (0x53).

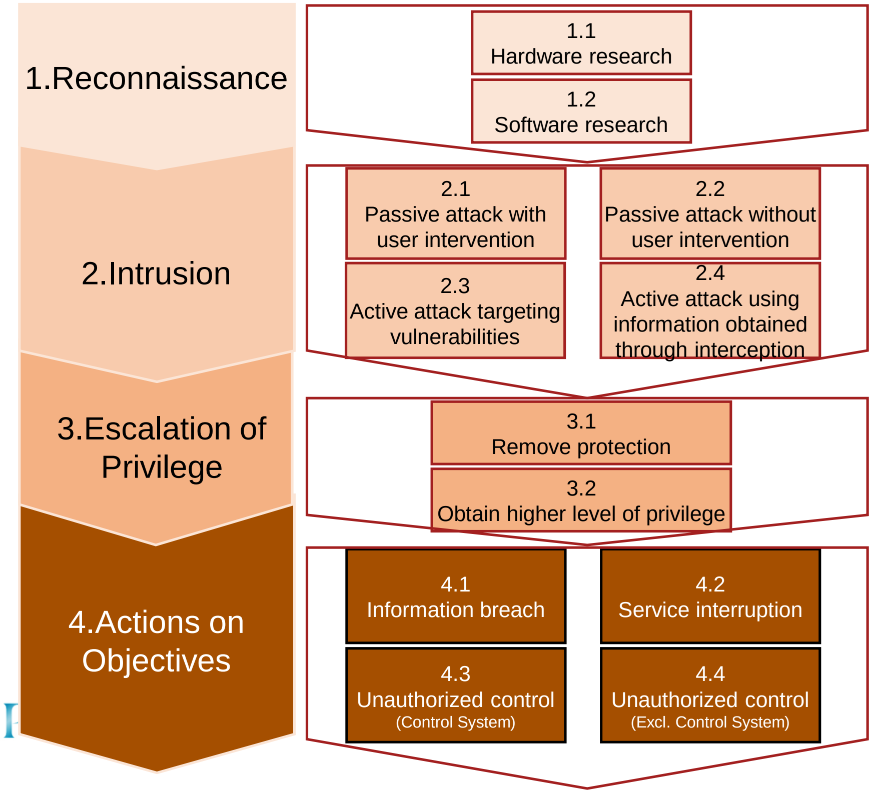
```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 0C B0 47 9C 27 F6 2D 93 3B EC 74 5A 8D A5 E3 98   ."Gœ'ö-";ìtZ.¥ã˜
0010h: B6 9F BD F7 C8 57 6B 89 C2 C7 6B E7 BC 6B 21 EA   ¶Ÿ½÷ÈWk‰ÂÇkç¼k!ê
0020h: 96 DC 0C D8 DD F4 B9 9B 64 CE 8F 8B 2A D0 8A 47   –Ü.ØÝô¹›dÎ.‹*ÐŠG
0030h: 2F 44 F7 D2 3F 45 06 4D 48 96 9E 6E 7D 7F 23 17   /D÷Ò?E.MH–žn}.#.
0040h: 49 C9 FE D1 F1 22 A0 34 20 C6 D0 5E DF DD E8 14   IÉþÑñ" 4 ÆÐ^ßÝè.
```

4. Overview and scope of Evaluation Guideline

Evaluation Items (based on actual hacking process)

Major Items

Medium Items



1.Reconnaissance

1.1 Hardware research

1.2 Software research

2.Intrusion

2.1 Passive attack with user intervention

2.2 Passive attack without user intervention

2.3 Active attack targeting vulnerabilities

2.4 Active attack using information obtained through interception

3.Escalation of Privilege

3.1 Remove protection

3.2 Obtain higher level of privilege

4.Actions on Objectives

4.1 Information breach

4.2 Service interruption

4.3 Unauthorized control (Control System)

4.4 Unauthorized control (Excl. Control System)

Evaluation Details

- Analyze system configurations, operating conditions of the vehicle and identify attack criteria.
  [Information collection to avoid randomness]
  ※Direct contact to the vehicle in reconnaissance phase

- Based on the conditions or information obtained in the reconnaissance phase, attempt intrusion through the wireless interface.
  ※Attacks attempted through wireless without direct contact to the vehicle from penetration phase onwards.

- After successful intrusion, obtain necessary rights to attack the vehicle by root break, jailbreak etc.
  ※Unnecessary to attempt in case higher level of privilege was obtained during intrusion phase.

- After succeeding in previous phases, attempt attacks that can cause actual impact to systems/user.
  [Identify impact caused by the discovered vulnerability]
  ※DoS (*Denial of Service*) attack from the external network shall be attempted even in case intrusion was unsuccessful.

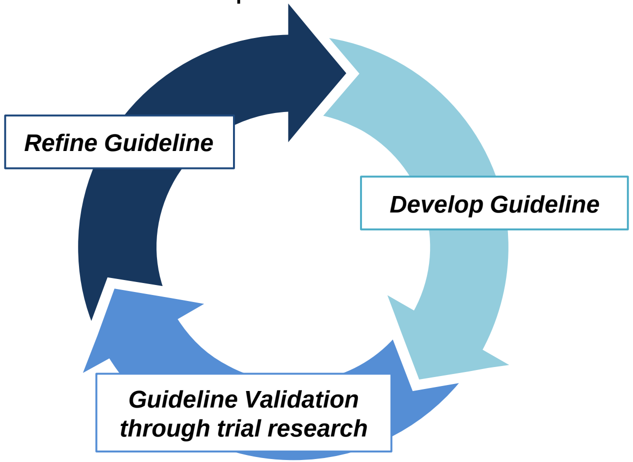
4. Overview and scope of Evaluation Guideline

Objective of the Trial Research

- The trial research was conducted to evaluate the validation of the guideline, and provide suggestions on vehicle security for the participants that provided the vehicle system for the FOT.

<table>
<tr><th>Validation of the guideline</th><th>Suggestion for the Participants</th></tr>
<tr><td>

Conduct evaluation on actual vehicle systems based on the items in the evaluation guideline to evaluate the validation of the guideline. The evaluation results will also be used to further improve the evaluation items.



</td><td>

From the hackers perspective, investigate vulnerabilities that could lead to security threats related to the tested vehicle system. Suggestions will be given to the participant in case problems were discovered that require improvement.

<u>Benefits for the Participants</u>

1. Clarify impact of the possible damage through simulated attacks to the hardware/software by highly skilled white-hackers
2. Obtain detailed procedures of the attack against the vehicle that can be reproduced by their own engineers
3. Obtain optimal countermeasures from both security quality and development cost point of view based on the actual impact clarified.

</td></tr>
</table>

5. FY2018 Evaluation Criteria and Guideline Update

- The judgement criteria for the evaluation in FY2018 are as follows. Each criteria will be validated through the results of the FOT and necessary changed will be reflected to the final guideline.

Evaluation condition	Method to realize reproducible evaluation	Verification method in FOT
1.Tester's Skill	• Identify necessary skills and conduct self-check by the testers prior to testing. • Include the checking process in the guideline	Cross-check validity of the skill check based on the results of evaluation items covered by each tester
2. Evaluation items	• Identify procedures described in the guideline	Evaluate variation of the evaluation items covered based on work evidence and results
3. Workload	• Conduct evaluation based on following set standard ➢ Evaluation period: 2 months (40 working days) ➢ Number of testers: 2	On precondition that No.1 & 2 were met, confirm whether the results meet the criteria for the participants
Evaluation Condition (Vehicle)	• Specify requirements	Assess variation of the vehicle systems provided for the FOT to confirm evaluable scope

Realize Reproducible Evaluation

Study/evaluate the results/issues/causes

Evaluation Result

Evaluation Criteria	【Reconnaissance Phase】 Reconnaissance attempts were unsuccessful after conducting evaluation fulfilling above mentioned skill and period, which confirms the security of the system as well as the reason. 【Intrusion Phase】 Intrusion attempts through every interface were unsuccessful after conducting evaluation fulfilling above mentioned skill and period.

Study/evaluate the results/issues/causes

Thank you