SIP-adus Workshop 2022

Session 6
Cyber Security

Threat Information Sharing and Proactive information collecting for Connected Cars

Shinichi Kan (PwC Consulting LLC)

12, October, 2022

INDEX

1. Introduction
2. Threat information sharing system
3. Proactive survey methodologies
4. Summary

1

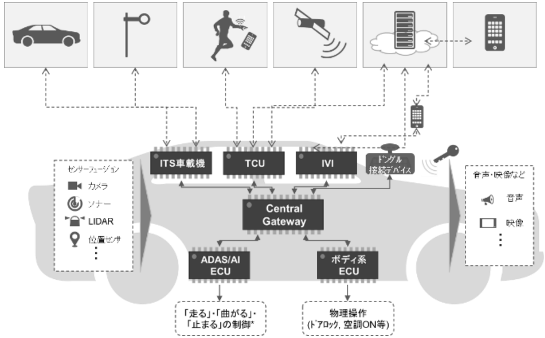
Introduction

Background and Research Objective

To deal with changes in the security environment due to the development of autonomous driving systems and the new international regulations, we are performing two research activities.

Changes in automotive security

Security risk in connected-system are increasing



New international regulation

UNECE WP29　UN-R155/R156

World forum for harmonization of vehicle regulations working Party 29(WP29)

Activity a. Development of IDS Evaluation Method and Guideline

Research Question : What are methods, procedures, environments required to evaluate in-vehicle IDS?

Activity b. Research on connected car threat intelligence and initial response support

Research Question :What kind of methods are available to collect and accumulate threat information for vehicles?
:What information required to support initial incident response for vehicles?

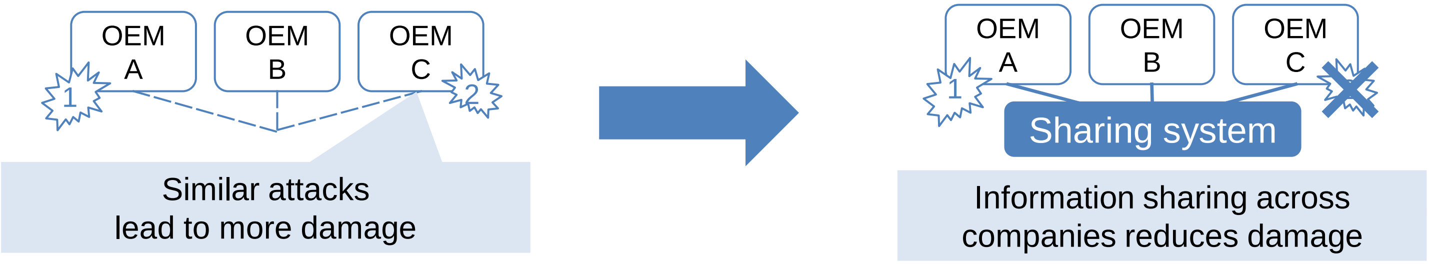
2

Threat information sharing system

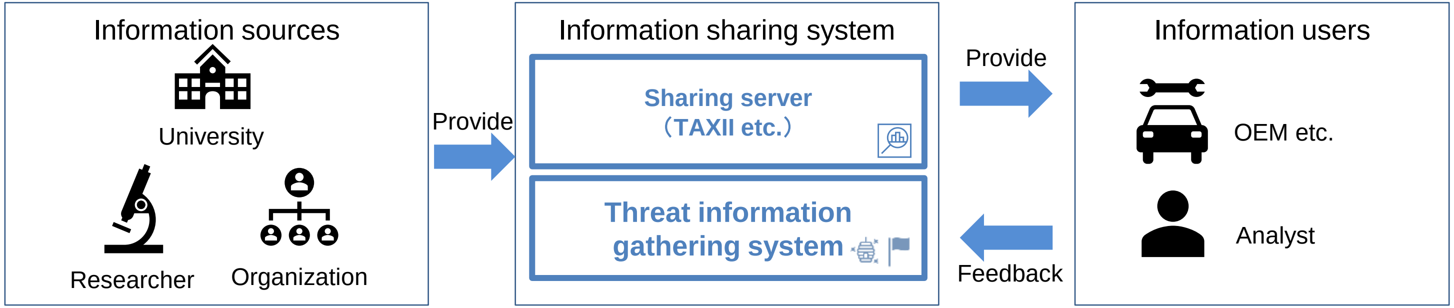
Threat information sharing system

Researching the basic design of a threat information sharing system to support post-shipment security measures in automotive industry.

- ✓ Advantage of information sharing system


OEM A
OEM B
OEM C
1
2
Similar attacks lead to more damage
OEM A
OEM B
OEM C
1
Sharing system
Information sharing across companies reduces damage

- ✓ Outline/schematic image of the system



Key features and methods for the sharing system

The key features and the methods we are considering to realize them are as follows.

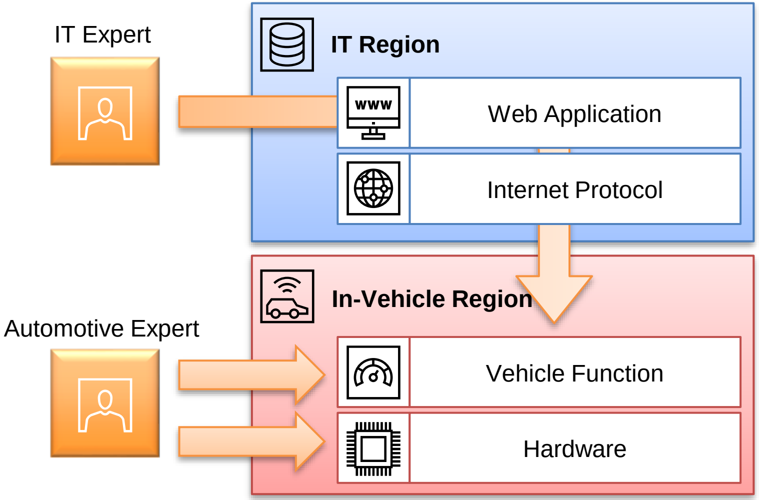
	Key Feature	Method	
1	Accumulating and sharing information effectively	- Structuring Threat Information - Common mechanisms for handling information	STIX TAXII
2	Understanding the status of companies and suppliers	- Creating a list of software that exists in company’s products and systems	S-BOM
3	Yielding useful information	- Collecting threat information proactively	Honeypot CTF

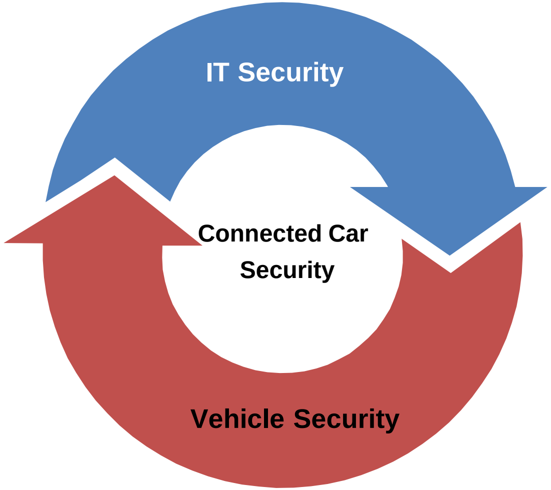
How to accumulate the threat information

Share | Utilize | Collect

We focused on STIX/TAXII as a candidate format for handling threat information in automotive industry, because it is widely used in IT field and can describe a variety of information.

Background: In accordance with the development of connected and automated vehicles, the use of IT and Web techniques becomes more common in automotive industry.

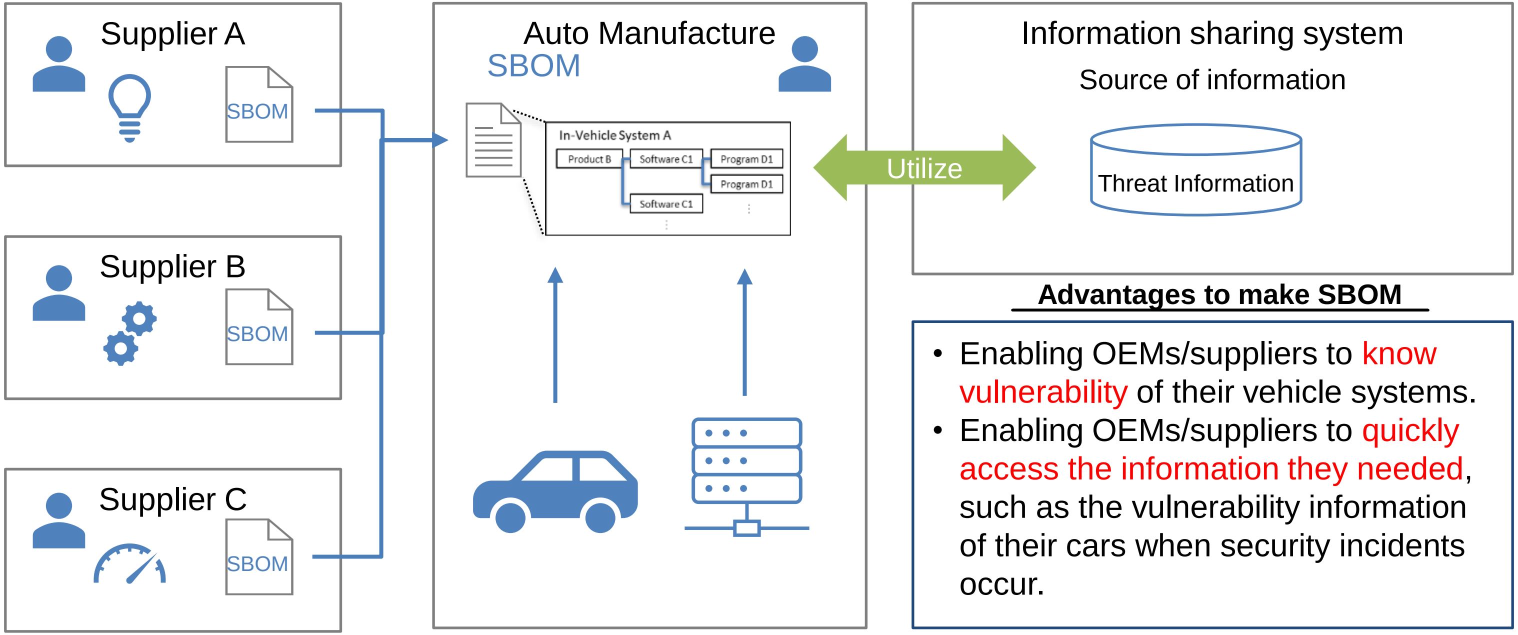




As the way to efficiently use threat information in the connected system, we focus on STIX/TAXII. STIX/TAXII is the most common in IT region and can describe a lot of threat information. STIX/TAXII enables us to address threats similar in IT region before they become apparent in the vehicle region.

How to utilize the threat information

By creating a list of the software in their products and systems, OEMs and suppliers can more smoothly analyze and utilize threat information collected/provided from the information sharing system.



Advantages to make SBOM

- Enabling OEMs/suppliers to know vulnerability of their vehicle systems.
- Enabling OEMs/suppliers to quickly access the information they needed, such as the vulnerability information of their cars when security incidents occur.

Proactive survey methodologies

Share | Utilize | Collect

Honeypot and CTF, the well-known ways to proactively survey threat information in the IT field.

They are adopted to obtain threat information for connected car systems.

Objective

- Establish a method for collecting and accumulating threat information in the automobile field.

Hypothesis

- In the IT field, various methods have been developed to actively collect threat information and elucidate attack methods. These are useful to build cyber intelligence.

→ It is natural to consider applying these methods to the automotive industry since these methods enable us to collect threat information, and reveal how to attack against the connected system.

(例)

Honeypot | CTF | OSINT | Bug bounty | Monitoring

Threat Information

- Attributes of cyber attackers / TTPs

Approach

- Consider attack patterns on connected systems and evaluate the possibility of collecting threat information through actual observation experiments using threat information collection methods in the IT field.

3

Proactive survey methodologies

Expectation on honeypot and CTF

The expectation of honeypot and CTF in this project is not to obtain specific threat, but to find out if are the methods beneficial to obtain car-related threat and organize them for future use.

Background:

- At the moment, attacks on connected cars are rare.
- In addition, no large-scale targeted attacks on connected cars, so-called attack campaigns, have been identified.

Honeypot and CTF are used to find out the following:

- Are there actually connected cars being accessed from the internet?
- Are there any devices that have been accidentally exposed to the internet?

- How do virtual attackers (CTF participants) attack cars?
- What motivates the (virtual) attackers?

CTF concept

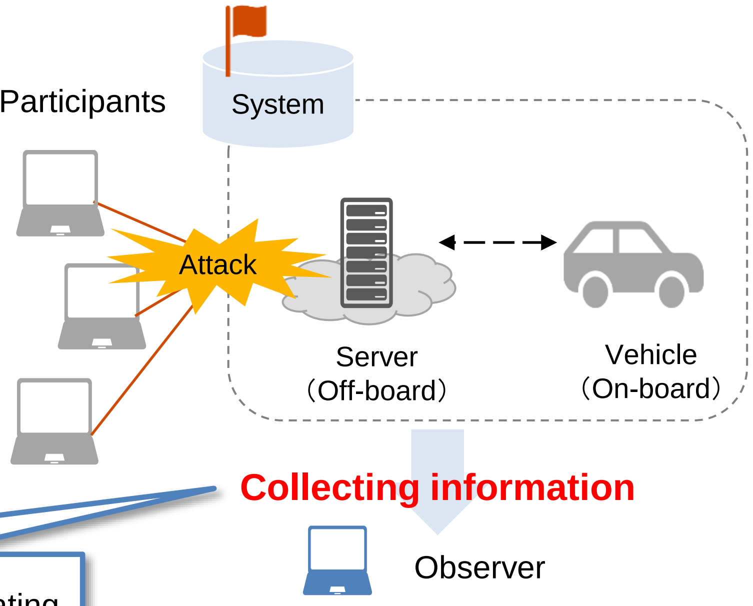
To detect an attack, we need to know the attack.

Analyzing what kind of activities against the servers are malicious (or gray) for connected vehicles and systems.
We set a target and ask participants to attack the system, and obtain knowledge for attack detections

Purpose	• What kind of attacks can be available against automotive connected system? • What kind of activities/behavior can be considered "vehicle targeted attacks"?
Plan	• Targeting vehicle control, acquisition of vehicle information, etc., the participant will attempt to attack the target system. • Obtain knowledge for quick detection of attacks based on observations of attackers' attack techniques and methods, etc.

In CTF…

It will be used for the development of honeypots and for creating decision criteria for analyzing attacks.

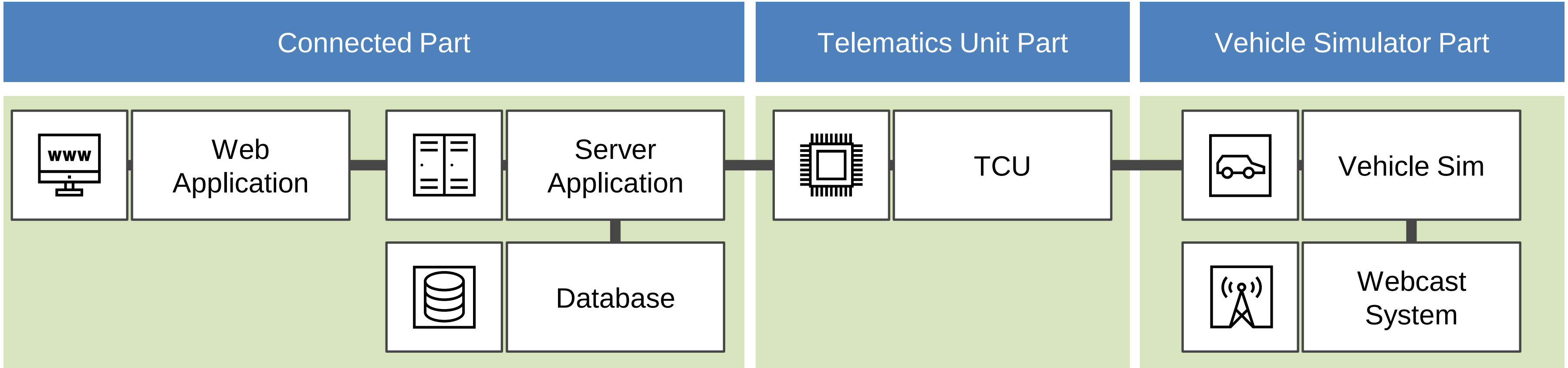


Collecting information

System configuration of the platform

We built a platform that replicates/mimics the vehicle, connected services (servers and user portals or apps) to hold a CTF with the goal of “Hijack the car”

The platform is a cyber attack verification system consisting of a connected server, telematics unit, and vehicle simulator.



Connected Part

Telematics Unit Part

Vehicle Simulator Part

Web Application

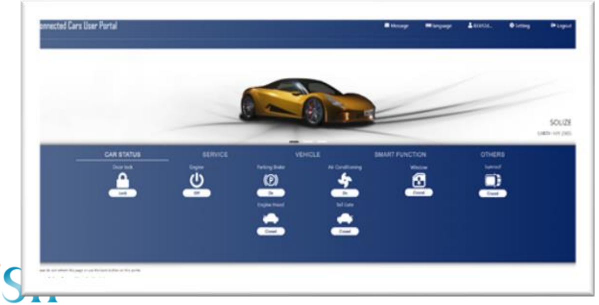
Server Application

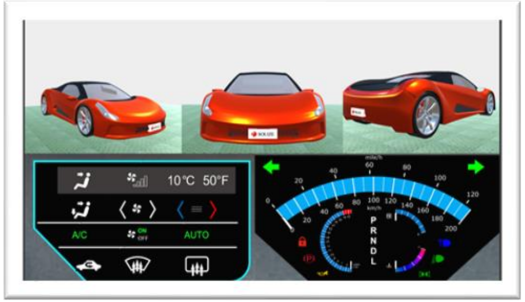
Database

TCU

Vehicle Sim

Webcast System





Platform Features

The platform implements the following main features as connected functions

Users can operate the vehicle (simulator) via connected services.

<table>
<tr><th colspan="5">Connected Service Part</th><th colspan="1">Telematics Unit Part</th><th colspan="2">Vehicle Simulator Part</th></tr>
<tr><td colspan="2">For vehicle owners Function</td><td colspan="2">Functions for Dealers</td><td colspan="2">Communication Functions</td><td colspan="2">Simulation</td></tr>
<tr><td colspan="2">Owner Portal Screen</td><td colspan="2">Management Portal Screen</td><td colspan="2">Send and receive SMS</td><td colspan="2">CG Model of Vehicle</td></tr>
<tr><td colspan="2">Door lock/unlock</td><td colspan="2">Vehicle Management</td><td colspan="2" rowspan="2">TCU communication protocol (SMS+HTTP)</td><td colspan="2">Body ECU</td></tr>
<tr><td colspan="2">turning on the light</td><td colspan="2">active test</td><td colspan="2">Chassis ECU</td></tr>
<tr><td colspan="2">horned pipistrelle</td><td colspan="2"></td><td colspan="2"></td><td colspan="2">Powertrain ECU</td></tr>
<tr><td colspan="2">Air conditioner operation</td><td colspan="2"></td><td colspan="2"></td><td colspan="2">Air conditioning and active testing</td></tr>
<tr><td colspan="2">Vehicle Information Display</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2">Engine start</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
</table>

4

Summary

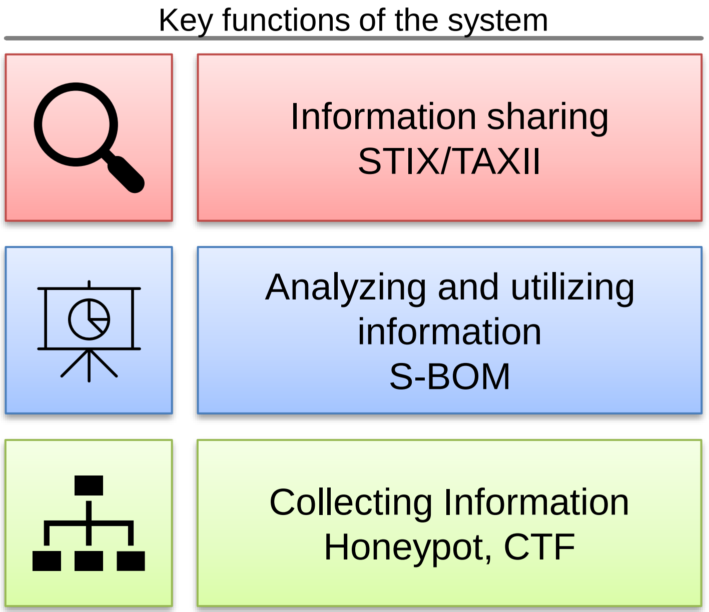
Summary

<Information sharing system>

- We are considering how to share, utilize and collect threat information smoothly and efficiently among industry groups and automobile manufacturers/suppliers.
- Discussions are underway to handover the outputs to an industry group.

<Proactive survey>

- In the automotive field, we proposed methods such as honeypots and CTFs to collect knowledge about new attack methods, in addition to collecting and accumulating existing threat information.
- We are also considering turning the CTF environment, which mimics the entire connected system, into a honeypot.



Key functions of the system

Information sharing
STIX/TAXII

Analyzing and utilizing
information
S-BOM

Collecting Information
Honeypot, CTF

Thank you

PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

A

Appendix

Functions in the sharing system

- We are considering how to share, utilize and collect threat information smoothly and efficiently among industry groups and automobile manufacturers/suppliers.
- Discussions are underway to transfer the deliverables to an industry group.

Key functions of the system	Advantages
Information sharing STIX/TAXII	• Enabling to share information smoothly without any discrepancy • Enabling to process information automatically.
Analyzing and utilizing information S-BOM	• Enabling to search threat information of a specific car, device and software. • Enabling to share information with and alert to not only OEM/suppliers themselves, but also to their related organizations, including suppliers
Collecting Information Honeypot, CTF	• Enabling to proactively collect new threat information, which emerges in daily, and to transmit useful information.