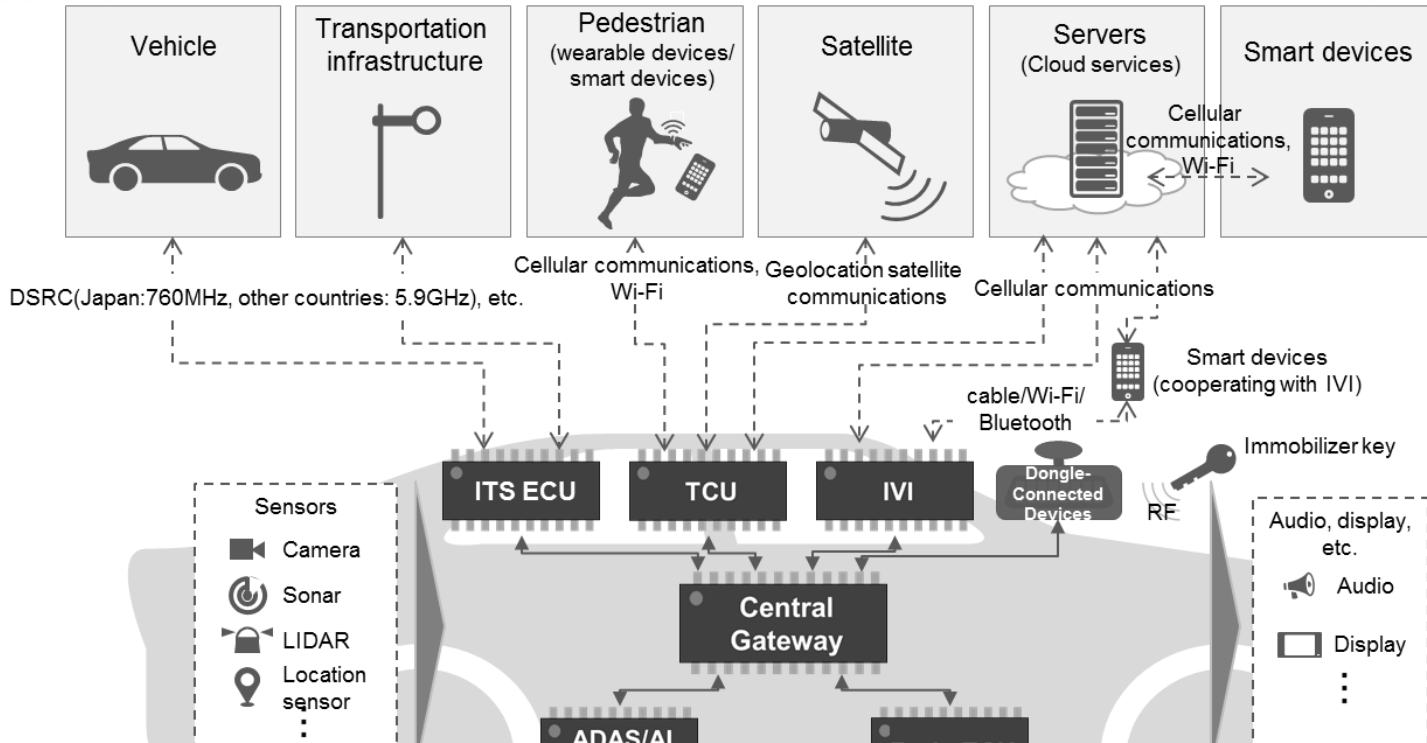


SIP-adus Workshop 2020

Cybersecurity

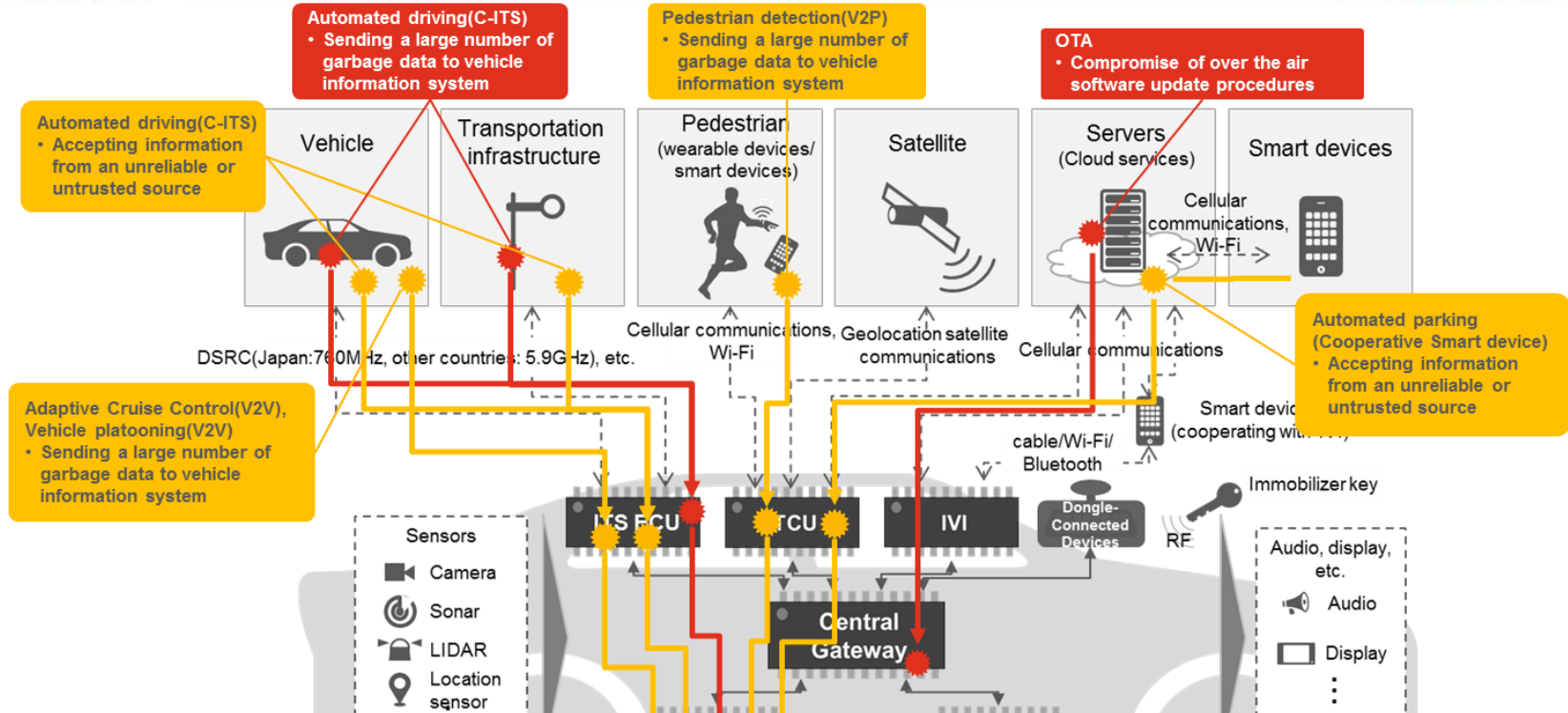
J-Auto-ISAC / TOYOTA Shigeru Uehara

System Configuration of Automated Driving



Automated Driving is realized by communication with external infrastructure

Many routes of intrusion exist



Attackers are constantly looking for new attack methods and trying to intrude. Under existing condition, we can not notice it until being attacked and damaged.

Monetary purpose

Unlike attacking the financial system and executing fraudulent remittance, Cyber attacks on vehicles are not directly linked to making money.

If the purpose is making money, the priority of attacking on vehicles would **not be high**.

(excluding special cases such as consignment crimes)

Pleasant purpose

Attackers may not take big risks in the situations where the technology of the crackdown authorities is improving. also,

The social interest in mischievous cyber attacks are low.

Pleasant purpose motivation **would be low** too.

Purpose of raising name recognition

In many cases,
Attackers are trying to show off their technical capabilities and make involved people understand the capabilities they own,
and, try to get benefit from them legally.

(e.g. Technical consultant contract of CS etc.)

This would be **the highest motivation** for
cyber attacks on vehicles.

From attacker's eye : Motivation to attack

additionally,

In many of this case, It's hard to forecast and defend because of the higher technical level attacks.

On the other hand, the attacker's purpose is "to raise their name recognition".

Therefore, They will reveal names, and will respond to our contact definitely.

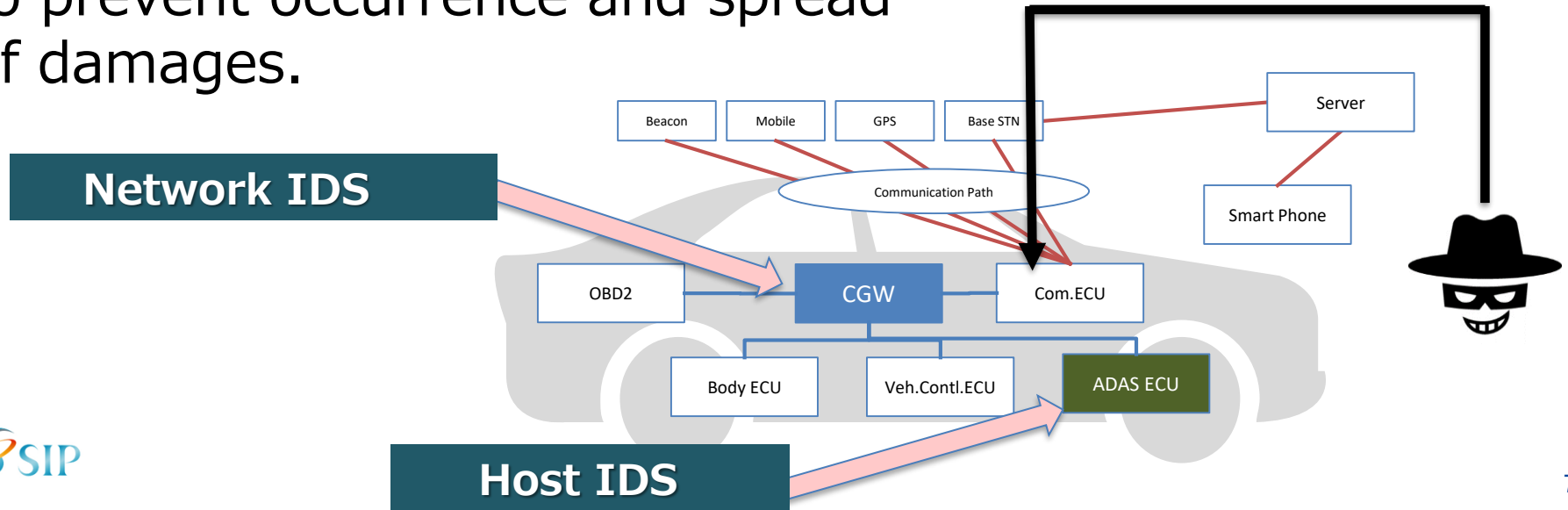
So, **If we can detect the attacks earlier and contact them,** and finally can build a good relationship with them, **We can take countermeasures without any damages.**

Defending side : What can be done

As defending side, we have few means that can promptly notice the intrusion.

It may only be **IDS** (Intrusion Detection System).

It is considered to be one of the few possible means to prevent occurrence and spread of damages.



Video Plenary Session

First, I will show you an IDS demo-video using test bed.

(Cooperated by PwC and TOYOTA)

After this, we have presentation about various points such as the future direction of IDS by 4 cybersecurity experts in the world.

IDS Test Bed



- ◆ Mr.Nishant Khadria

Senior Manager,Risk Advisory, Deloitte Germany

- ◆ Mr.Robert Shein

Senior Manager,Consulting-Technology, PwC USA

- ◆ Mr.Shigeyuki Kawana

Leader of Elec.Safety sub-committee, JAMA

- ◆ Prof.Tsutomu Matsumoto

Yokohama National University

SIP-adus Workshop 2020

Let's start our session