Secure Software Update for ITS Communication Devices in ITU-T Standardization

Masashi, Eto

Senior Researcher, Cybersecurity Laboratory,
Network Security Research Institute, NICT, Japan

National Institute of Information and Communications Technology

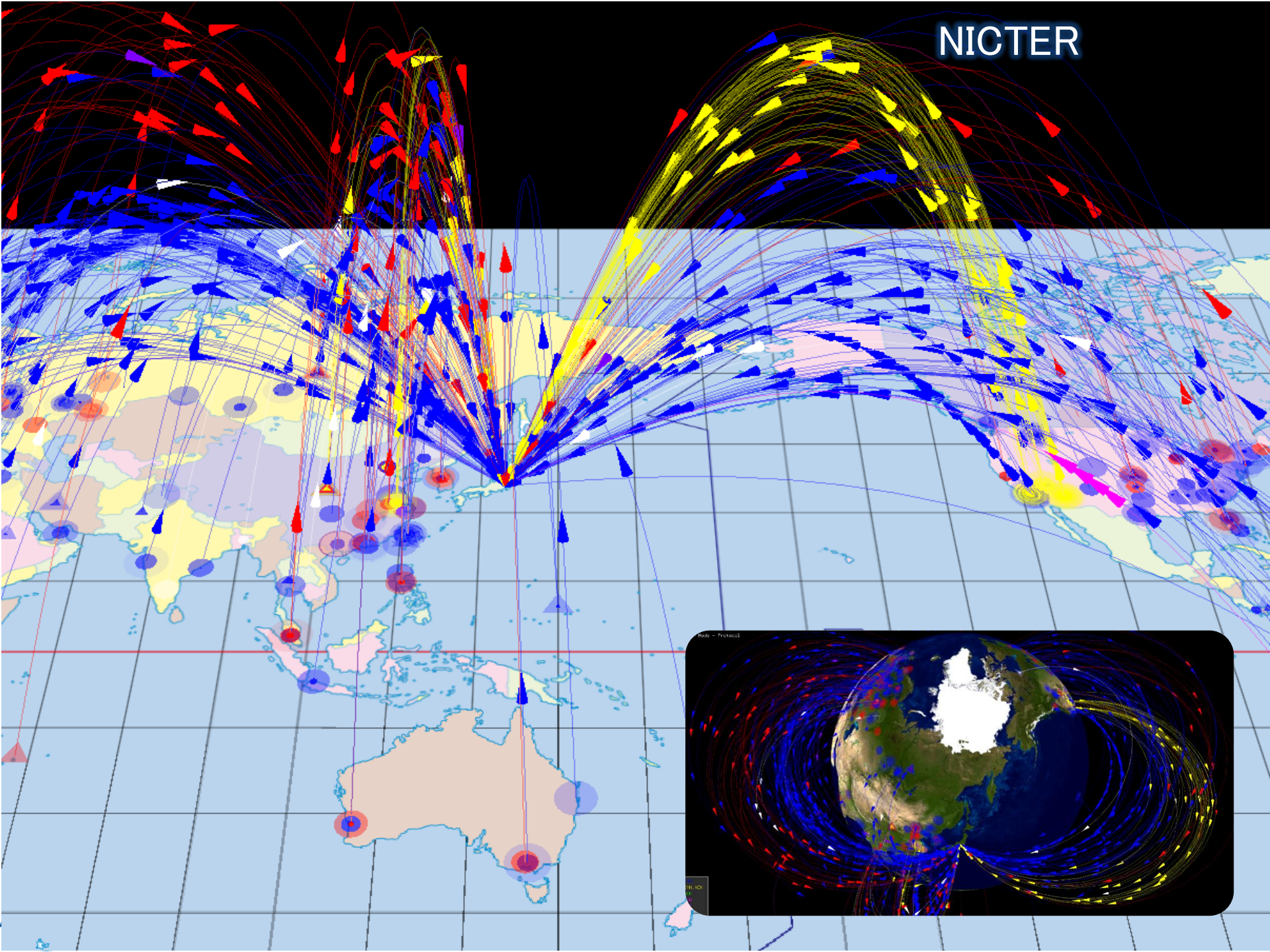
Outline

- **Background**
  - Threats against networked embedded devices
  - Necessity of remote update (maintenance) of vehicle
- **General remote update procedure and threat analysis**
- **An approach of international standardization in ITU-T**
  - Introduction of "Secure software update capability for ITS communications devices"
- **Conclusion**

National Institute of Information and Communications Technology

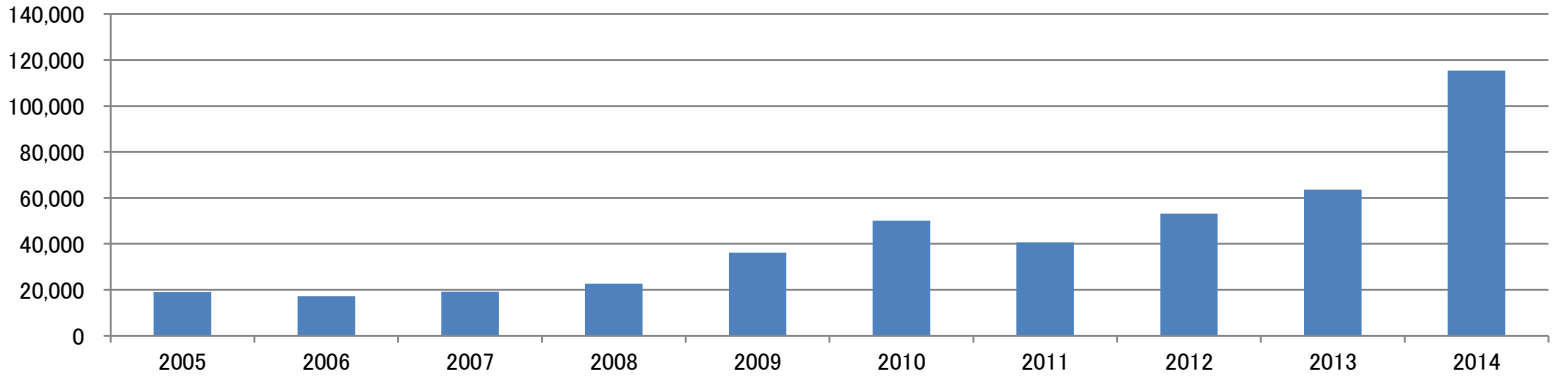
Background

National Institute of Information and Communications Technology


NICTER

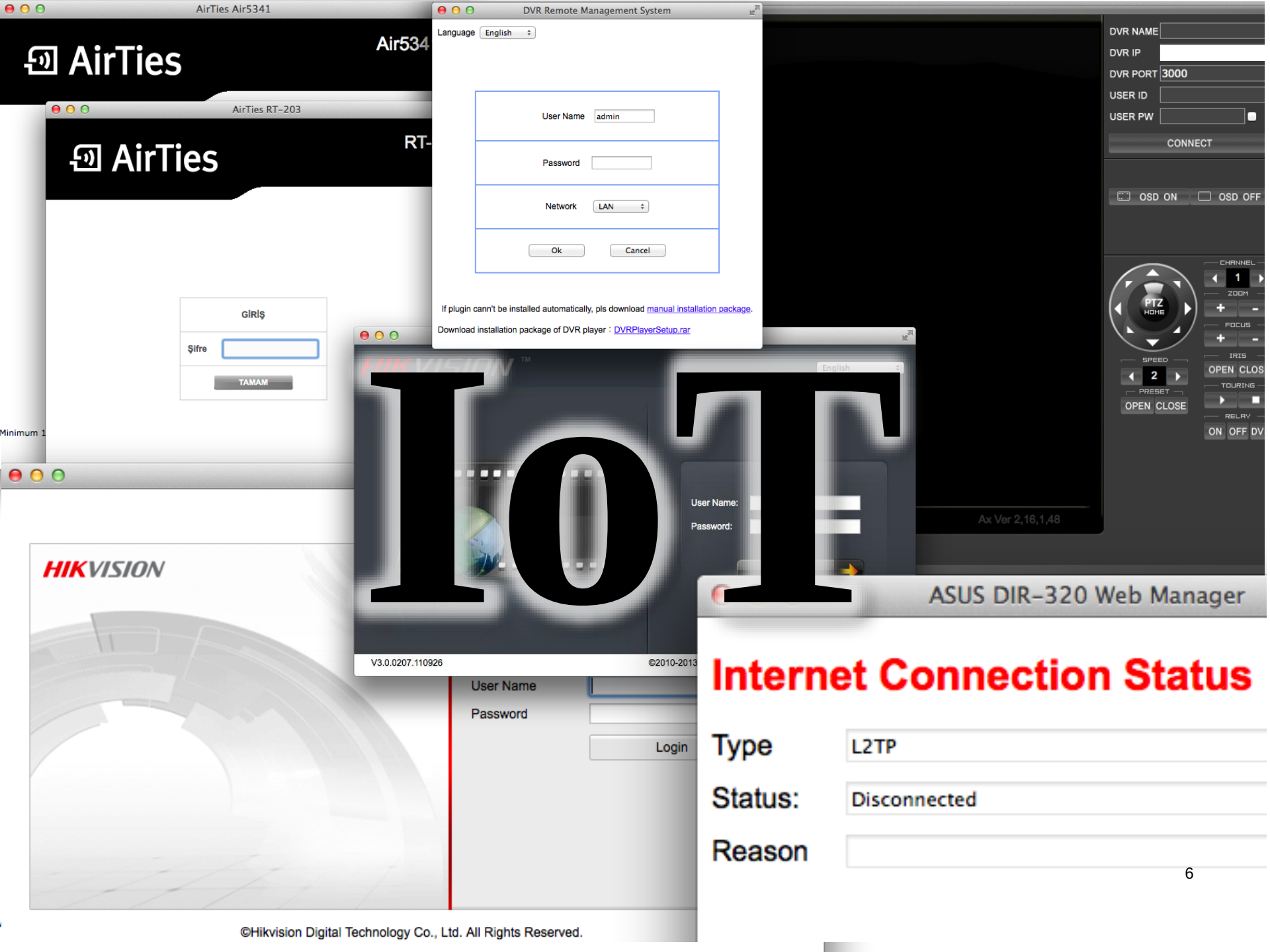
Stats of Darknet Traffic

Year	Number of packets par year	Number of IP address For darknet	Number of packets par 1 IP address per year
2005	0.31 billion	16 thousands	19,066
2006	0.81 billion	100 thousands	17,231
2007	1.99 billion	100 thousands	19,118
2008	2.29 billion	120 thousands	22,710
2009	3.57 billion	120 thousands	36,190
2010	5.65 billion	120 thousands	50,128
2011	4.54 billion	120 thousands	40,654
2012	7.79 billion	190 thousands	53,085
2013	12.9 billion	210 thousands	63,655
2014	**25.7 billion**	240 thousands	**115,323**

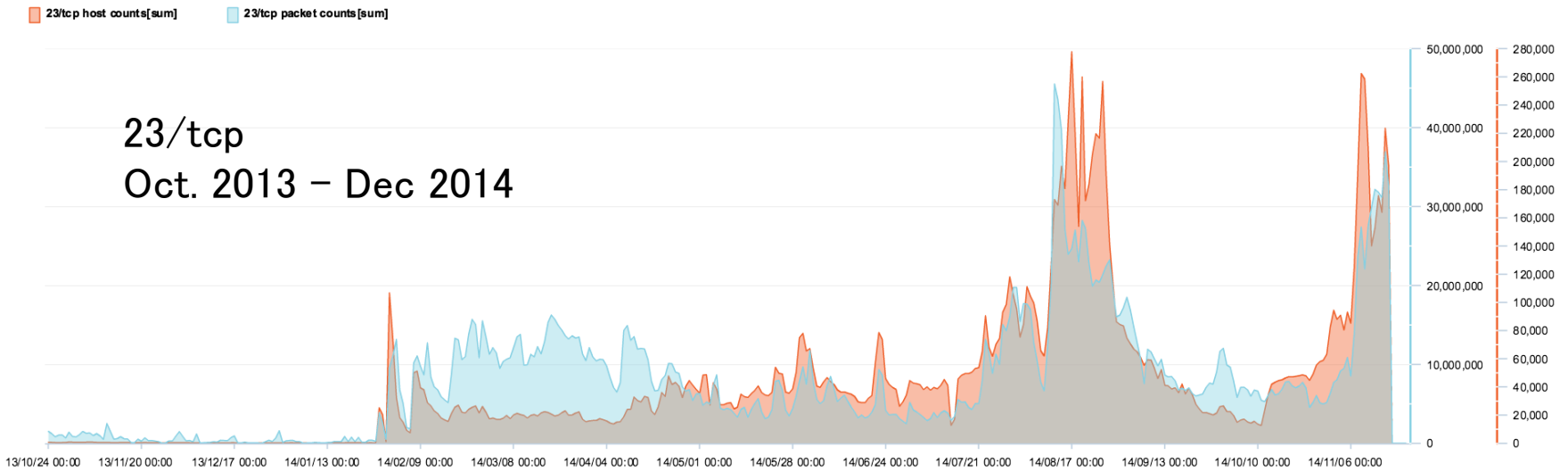


Number of packets par 1 IP address per year

National Institute of Information and Communications Technology


AirTies Air5341
AirTies
AirTies RT-203
AirTies
GİRİŞ
Şifre
TAMAM
DVR Remote Management System
Language English
User Name admin
Password
Network LAN
Ok
Cancel
If plugin cann't be installed automatically, pls download manual installation package.
Download installation package of DVR player : DVRPlayerSetup.rar
DVR NAME
DVR IP
DVR PORT 3000
USER ID
USER PW
CONNECT
OSD ON
OSD OFF
PTZ
HOME
CHANNEL
ZOOM
FOCUS
IRIS
SPEED
PRESET
TOURING
RELAY
OPEN
CLOSE
ON
OFF
IoT
User Name:
Password:
Ax Ver 2,16,1,48
V3.0.0207.110926
©2010-2013
HIKVISION
User Name
Password
Login
©Hikvision Digital Technology Co., Ltd. All Rights Reserved.
ASUS DIR-320 Web Manager
Internet Connection Status
Type L2TP
Status: Disconnected
Reason

23/tcp Scan from Embedded Device



- Infected Devices
  - ✓Home Router
  - ✓Web Camera
  - ✓NAS: Network Attached Storage etc. etc...

National Institute of Information and Communications Technology

IoT Devices Attacked JP

Investigated by Yoshioka Lab in YNU

Wireless Router

Food Processing Machine

Confirming now

Wifi Audio Receiver

Black Box Media Player

Wireless Router

Radio Bridge Equi

Most of these devices are running on embedded OS with opened port for management (23, 80, 8080/tcp).

IP– Camera

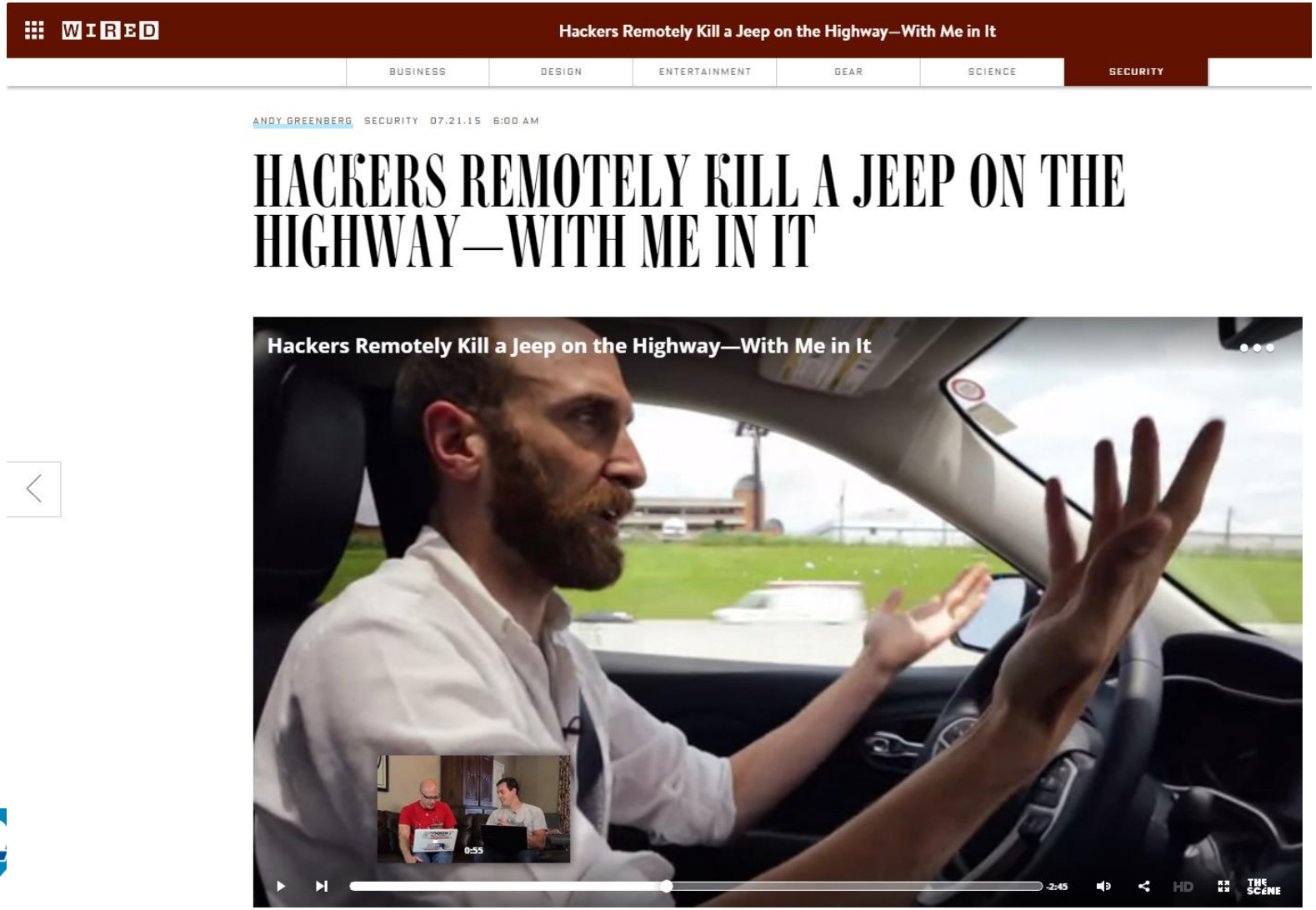
Heat Pump

OfficeServ System

YOKOHAMA National University YNU

Networked vehicle is not the exception!

- Networked vehicle also might have vulnerable opened port to be exploited by remote attackers.



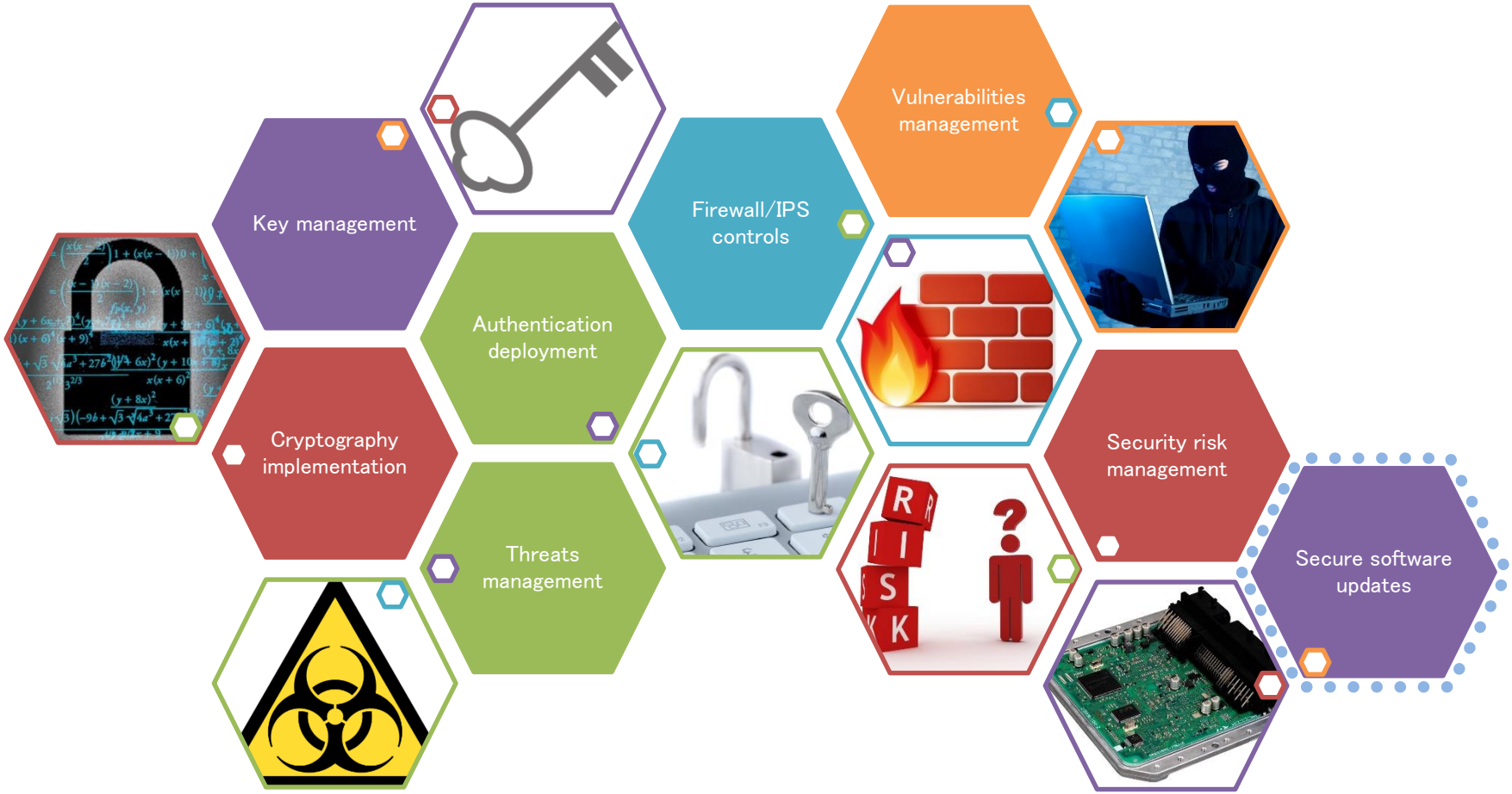
Remote exploitation against Jeep Cherokee (cont.)

- **Research activity by two hackers**
  - Presented at Black Hat USA 2015 (5-6, Aug)
    - "Remote Exploitation of an Unaltered Passenger Vehicle"
    - Charlie Miller, Security Engineer, Twitter
    - Chris Valasek, Director of Security Intelligent at IOACTIVE, INC.

- **Demonstration of attacks against FIAT Chrysler's Jeep Cherokee**
  - Remote exploit attack against port 6667/tcp of an Internet-connected device (UConnect)
  - Remotely controlled the vehicle on the highway
    - Abuse a steering wheel
    - Abuse brake and accelerator
    - On/Off of the engine

What security controls should be considered!

- There are many security controls which should be considered for future car environment



National Institute of Information and Communications Technology

Necessity of remote update (maintenance) of vehicle

- **Improvement of vehicle**
  - Software modules inside ECUs must be frequently updated
    e.g.) bug fix, performance and security improvement

- **Cost Reduction**
  - Failure of the software accounts for about 30% of the current recall of the cars.

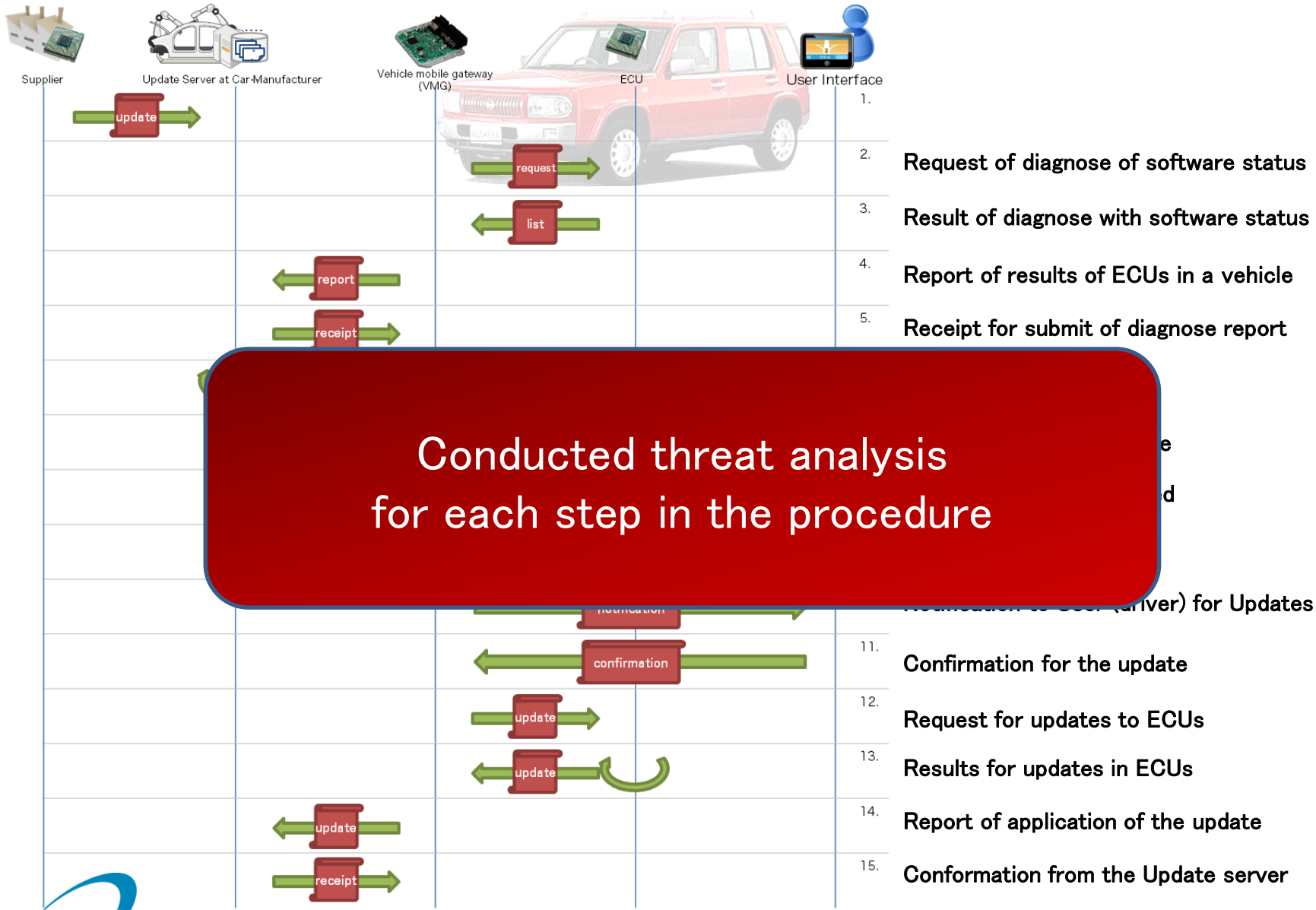
- **Automotive industries and users expect benefit from the remote update service in secure manner**

National Institute of Information and Communications Technology

General remote update procedure and threat analysis for networked vehicle

National Institute of Information and Communications Technology

Model data flow of remote software update



Conducted threat analysis
for each step in the procedure

National Institute of Information and Communications Technology

Threat analysis: example case

3. ECUs generate a software list and submit it to the Vehicle mobile gateway.

Impersonation of ECU

- ! Improper software information is uploaded to VMG
- ! DoS attack against VMG by sending forged data (e.g., enormously huge data)

Impersonation of VMG

- ! Software information on every ECU in the vehicle is improperly collected

Tampering / eavesdropping / replay of a message

- ! Improper software information is uploaded to VMG
- ! Software information on every ECU in the vehicle is improperly collected
- ! DoS attack against VMG by sending forged data (e.g., enormously huge data)

An approach of international standardization in ITU-T

Introduction of “Secure software update capability for ITS communications devices”

National Institute of Information and Communications Technology

Development of an ITU-T Recommendation

- **ITU-T: International Telecommunication Union, Telecom sector**
  - SG17: Responsible for security standards
- **Title of Recommendation**
  - "Secure software update capability for ITS communications devices" (X.itssec-1)
- **Purpose**
  - to provide common methods to update the software by a secure procedure including security controls and protocol definition
  - The adoption of the Recommendation is not mandatory for automotive industries, but the Recommendation would be a guideline of the baseline security for networked vehicle.
- **Editors**
  - Masashi Eto (NICT)
  - Koji Nakao (KDDI/NICT)

National Institute of Information and Communications Technology

Security controls for the software update

- ✓ **Message verification**
  - Threats: tampering, eavesdropping and replaying of messages
  - Measure: message verification mechanism based on Message Authentication Code (MAC) or digital signature method

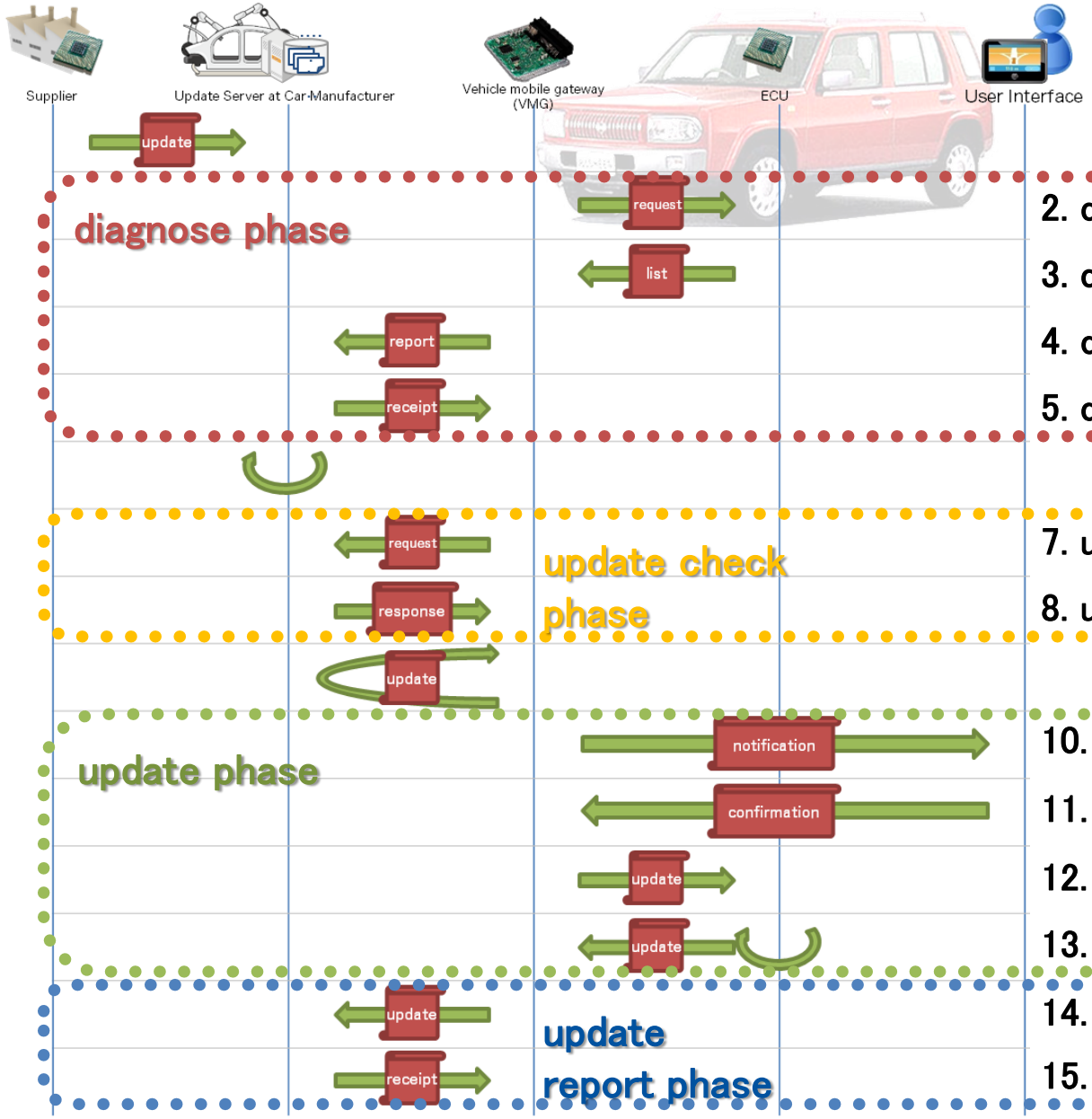
- ✓ **Trusted boot of ECUs**
  - Threats: tampering of software in ECU
  - Measure : hardware Security Module (HSM) to verify software modules in ECUs' boot sequences

- ✓ **Authentication of communication entity**
  - Threats: impersonation of the entities
  - Measure : authentication of both client and server of each communication based authentication protocol such as SSL/TLS

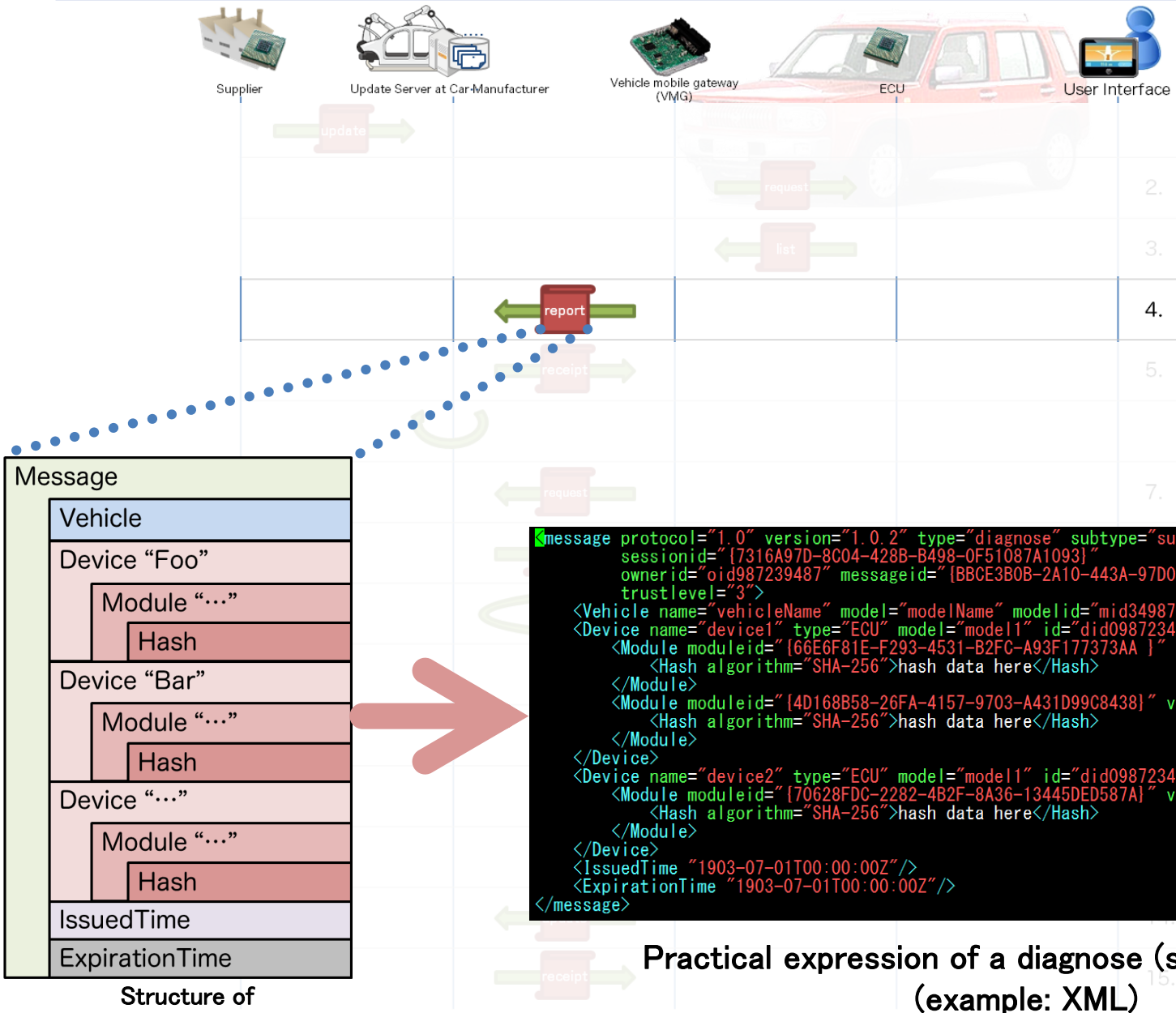
- ✓ **Message filtering**
  - Threats: DoS attack against VMG or update server
  - Measure : message filtering based on white listing of senders and frequency limitation of received messages, etc.

- ✓ **Fault tolerance**
  - Threats: DoS attack against VMG
  - Measure : measures such as auto-reboot for recovery of normal state, safe suspension of operation should be taken if something irregular is detected on the operation of VMG.

Protocol definition (Phases)



Example of a message: diagnose (submit)



Structure of diagnose (submit) message

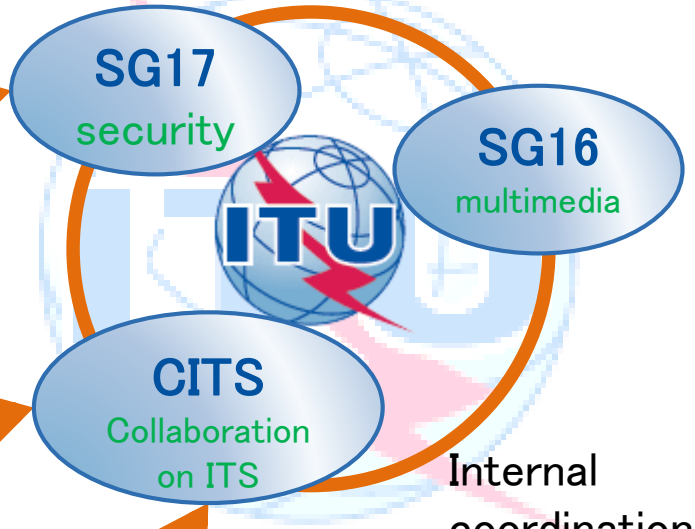
```
<message protocol="1.0" version="1.0.2" type="diagnose" subtype="submit"
         sessionid="{7316A97D-8C04-428B-B498-0F51087A1093}"
         ownerid="oid987239487" messageid="{BBCE3B0B-2A10-443A-97D0-EF4650457422}"
         trustlevel="3">
    <Vehicle name="vehicleName" model="modelName" modelid="mid34987130" vehicleid="vid0987234"/>
    <Device name="device1" type="ECU" model="model1" id="did0987234">
        <Module moduleid="{66E6F81E-F293-4531-B2FC-A93F177373AA }" version="1.3.23.0" nextversion=""/>
            <Hash algorithm="SHA-256">hash data here</Hash>
        </Module>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}" version="2.4.34.0" nextversion=""/>
            <Hash algorithm="SHA-256">hash data here</Hash>
        </Module>
    </Device>
    <Device name="device2" type="ECU" model="model1" id="did0987234">
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}" version="3.5.45.0" nextversion=""/>
            <Hash algorithm="SHA-256">hash data here</Hash>
        </Module>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

Practical expression of a diagnose (submit) message (example: XML)

Collaboration with industry

- This activity is highly required to collaborate with automotive industries and other standardization organizations (SDOs).
- ITU-T kindly ask automotive industry in the world to provide us their suggestions so that it can make the Recommendation practically useful for automotive industry.

International SDOs



Internal coordination

Car manufactures and suppliers

National Institute of Information and Communications Technology

Current status and the future plan

- **Current status**
  - Draft Recommendation of X.itssec-1
    - achieved a certain level of quality through discussions with some car manufactures and suppliers at the ITU-T SG17 meeting in Sep. 2015.
  - Requesting for comments
    - The draft Recommendation is under review within this year by ITU-T CITS (Collaboration on ITS Communication Standards) where relevant parties are involved.

- **Future steps**
  - Jan, 2016: ITU-T SG17 Interim meeting (Q.6) at Seoul
    - make disposition of comments from automotive industries, etc.
  - Mar, 2016: ITU-T SG17 meeting at Geneva
    - To be determined as a Recommendation

Conclusion

- **Threat analysis in a general software update procedure**
  - Impersonation of entities, tampering of software in ECU, etc.,

- **Introduction of ITU-T draft Recommendation X.itssec-1**
  - "Secure software update capability for ITS communications devices"
    - Threat and risk analysis
    - Security controls against threats of vehicles
    - Protocol definition and data format of a practical procedure
  - **The standardization activity on this topic should be accelerated in corporation with automotive industries. This should be also supported by establishment of related regulation for each country and/or region.**

National Institute of Information and Communications Technology

Thank you for your attention!

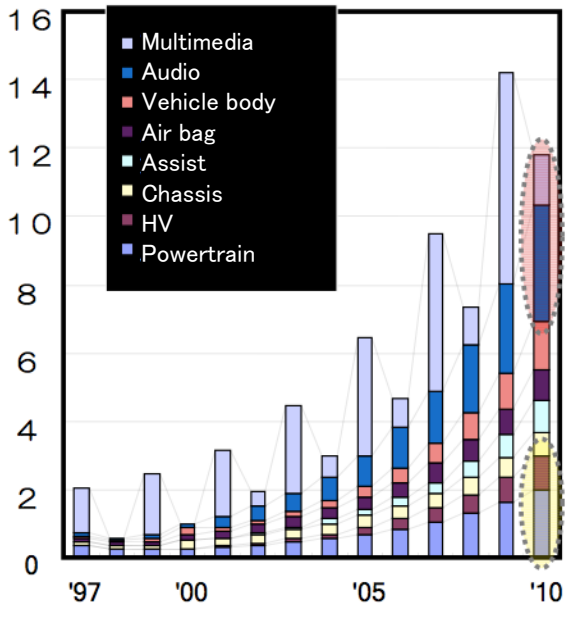
National Institute of Information and Communications Technology

Extra slides

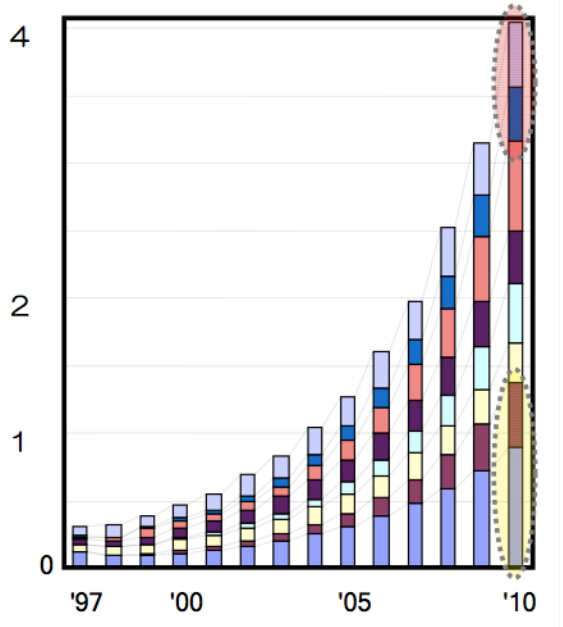
Computerization of vehicle

50%	100	100 million	5	2 miles
Proportion of electronic components of car production costs	Number of ECUs (Electronic Control Unit) in luxury models	Number of program lines of car software	Number of networks in a car (average)	Length of cable in a car

Software Development Volume



Software Development Cost

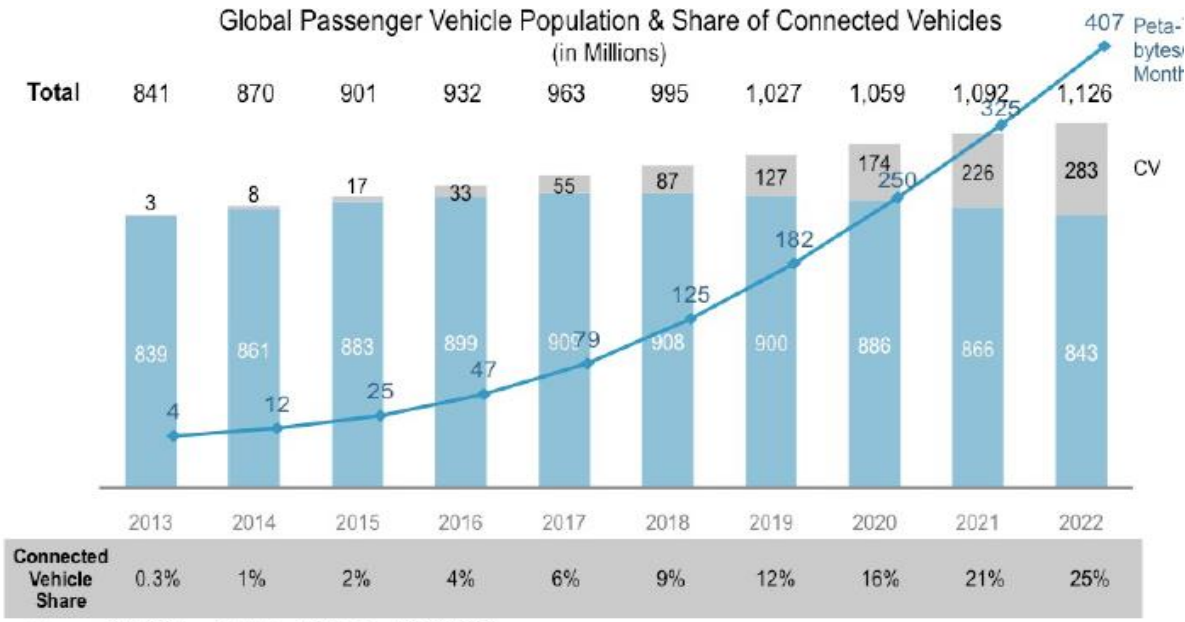


National Institute of Information and Communications Technology

Connected Vehicles

- Internet connection (LTE, 3G, Wi-Fi, Bluetooth …)
  - via customer's smartphone, SIM embedded in the vehicle, etc.

- Autonomous car
  - Control engines and brakes based on the information from roadside infrastructure as well as car-mounted sensors, cameras, and radars



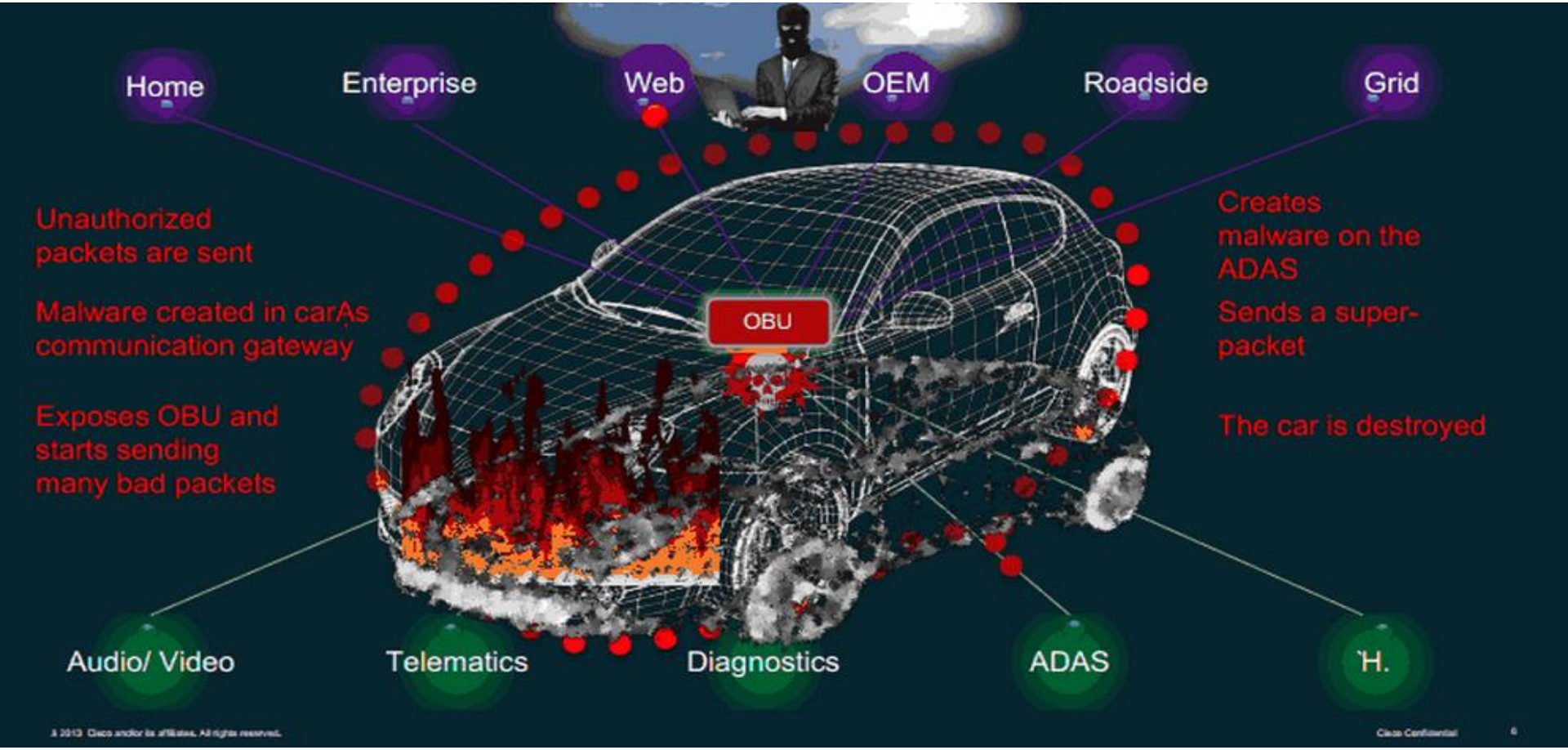
[1] Average of 1.5 GB/month/vehicle, 1 Petabyte = 1,048,576 GB

Sources: Cisco IBSG, 2011, based on data from U.S. Department of Transportation, iSupply, McKinsey & Company

National Institute of Information and Communications Technology

Threats against networked vehicle

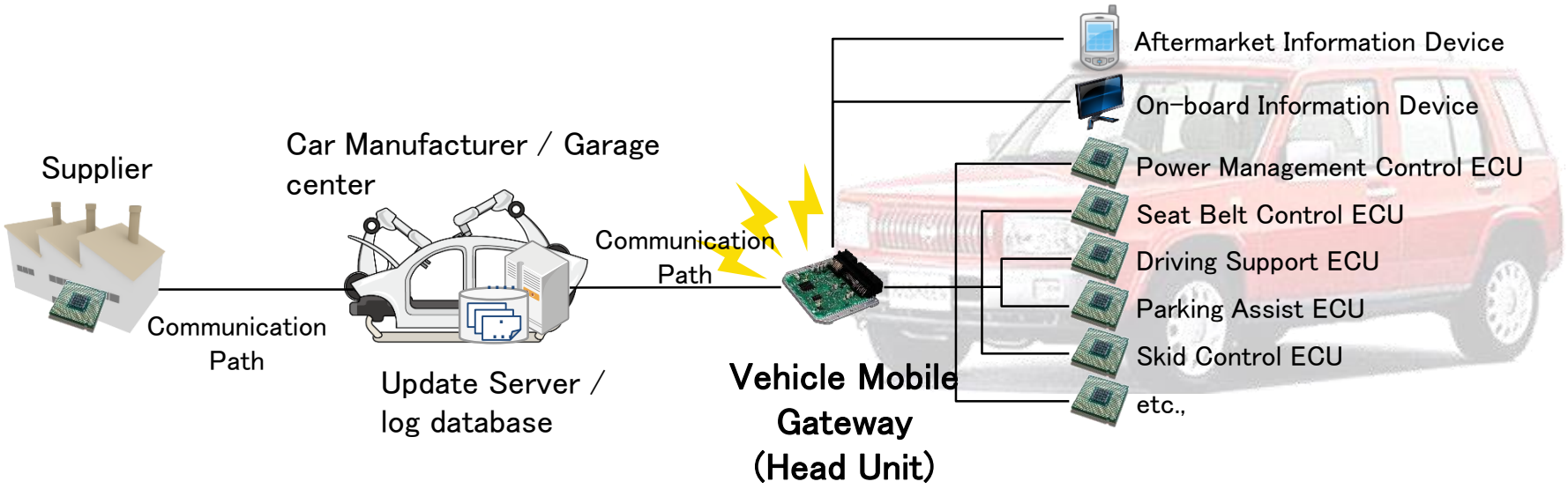
- More Attacks Surfaces!　Each New Connection or Device Adds a Potential Target!!



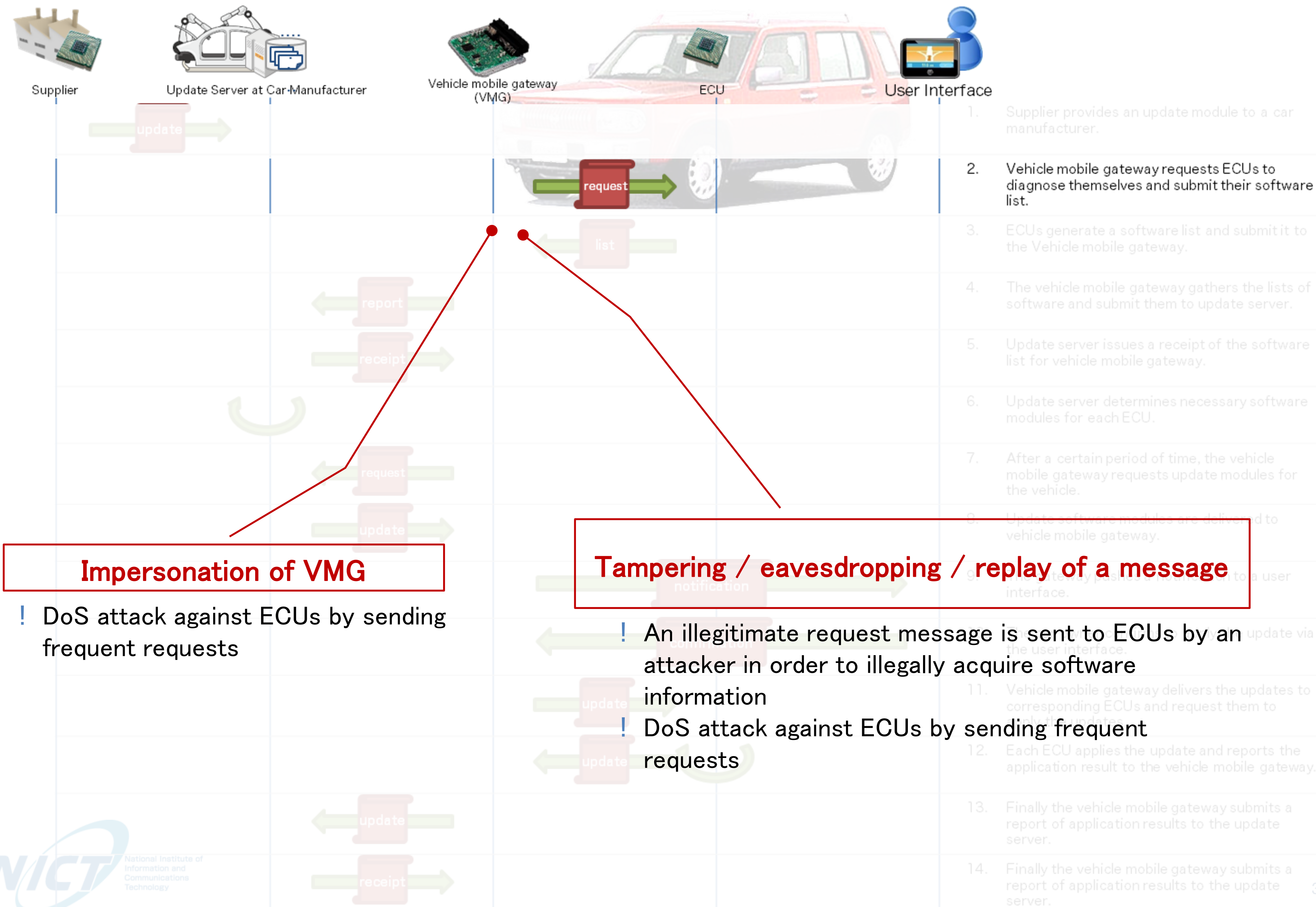
http://gigaom.com/2013/08/06/ciscos-remedy-for-connected-car-security-treat-the-car-like-an-enterprise/

National Institute of Information and Communications Technology

General model of networked vehicle



Threat analysis: example case 1



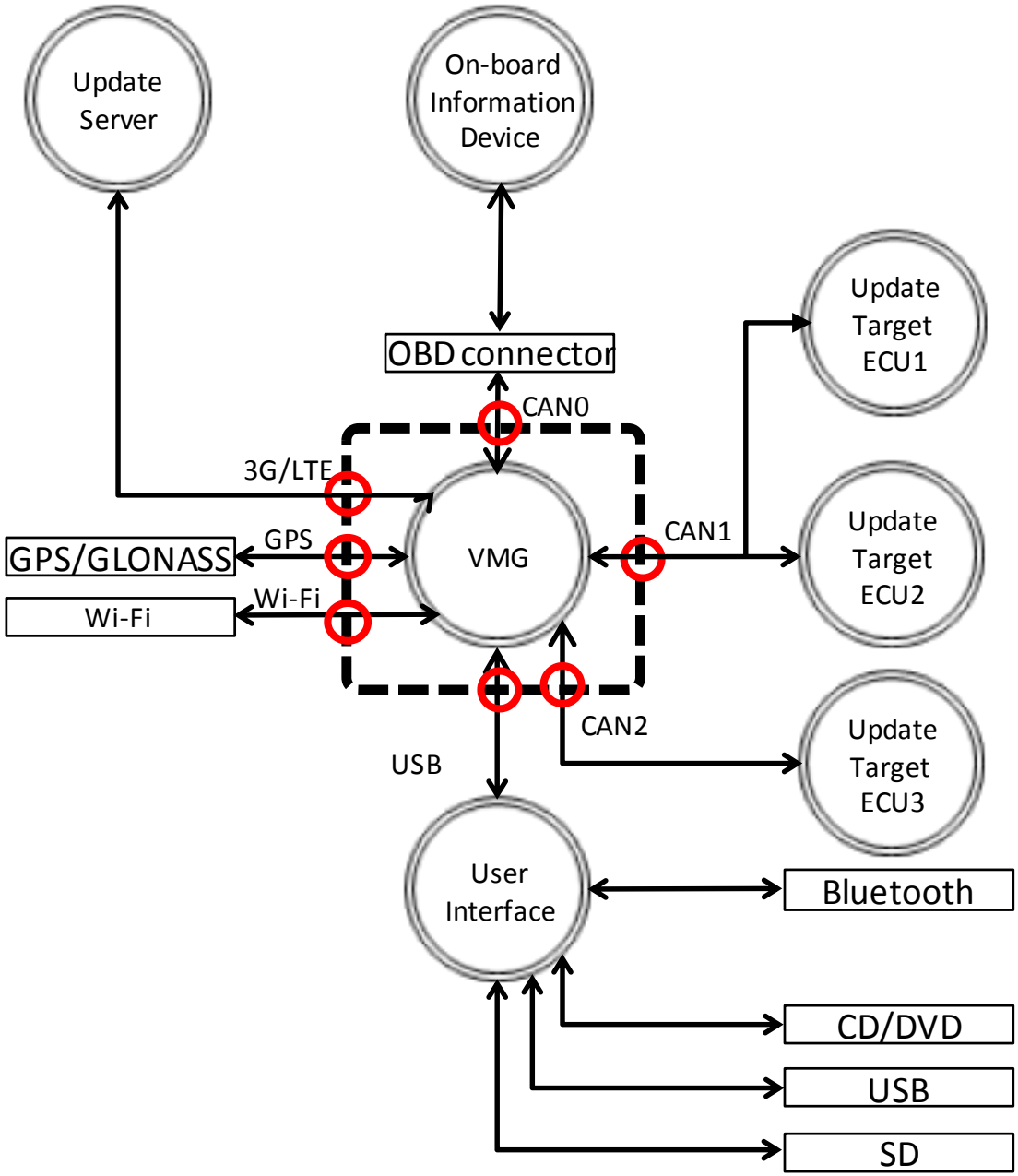
Impersonation of VMG

- DoS attack against ECUs by sending frequent requests

Tampering / eavesdropping / replay of a message

- An illegitimate request message is sent to ECUs by an attacker in order to illegally acquire software information
- DoS attack against ECUs by sending frequent requests

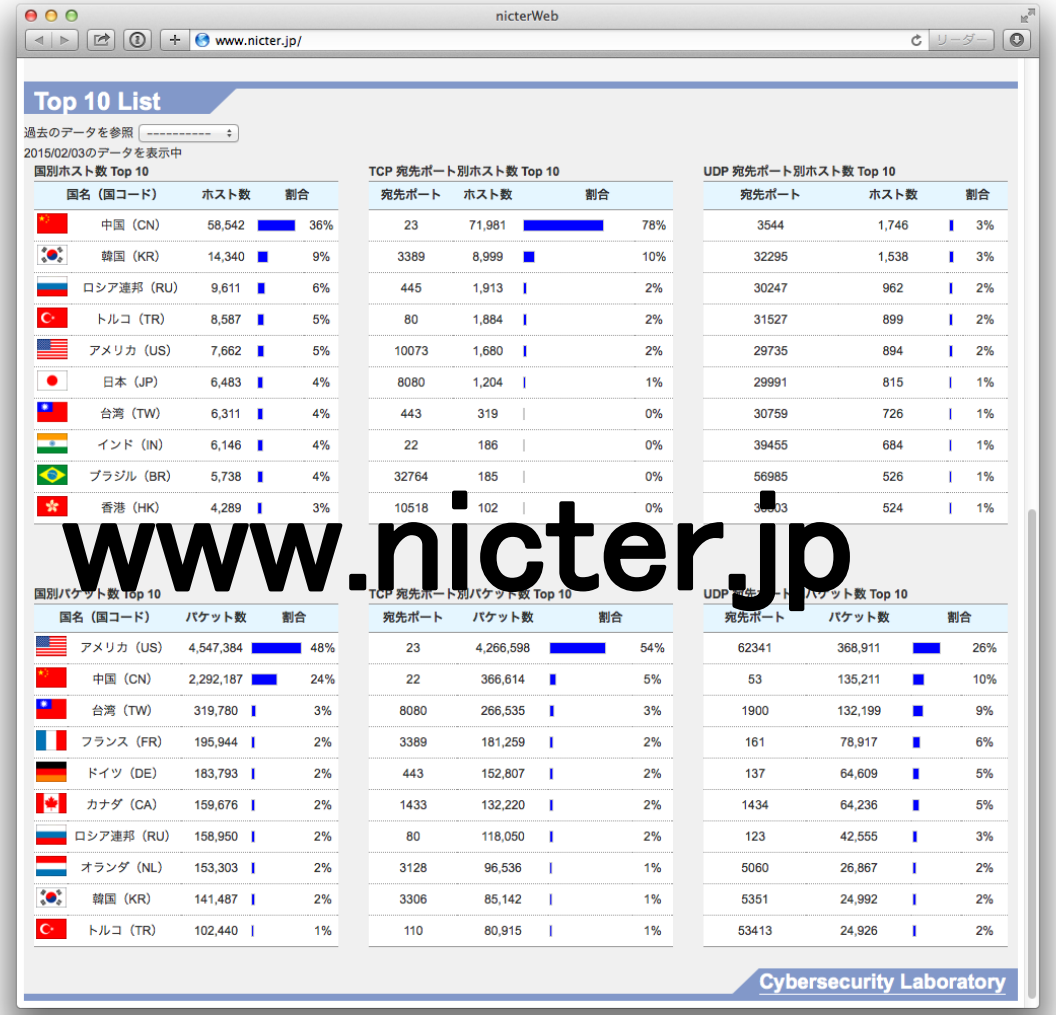
The model of the TOE (Target of Evaluation)



Threats for TOE with risk score more than a certain high value

#	Label	Who	When(phase)	Why	Where/What	Risk score
1	T.DoS-Functions-From-OBD-Device	third party maintenance factory staff	normal operation maintenance	intentionally	For asset functions of VMG, it impersonates an OBD connector connection device, sends a huge amount of data, interferes this function.	6.6
2	T.Mulfunction-Functions-From-OBD-Device	third party maintenance factory staff	normal operation use / maintenance maintenance	intentionally	For asset functions of VMG, impersonates an OBD connector connection device, sends unauthorized data, causes a malfunction of this functionality	6.6
3	T.MissDoS-Functions-From-OBD-Device	vehicle dealer staff maintenance factory staff	maintenance	accidentally	For asset functions of VMG, sends a huge amount of data or unauthorized data from OBD connector connection device by mistake, and causes a malfunction of this functionality	6.6
4	T.DoS-Functions-From-ECU	third party maintenance factory staff	normal operation/ use / maintenance maintenance	intentionally	For asset functions of VMG, it uses reverse engineering of the same product as the ECU firmware connected to CAN0-2, update ECU firmware connected to CAN0-2 to an unauthorized firmware, in this way, sends a huge amount of data from ECU connected to CAN1-5, interferes this functionality	5.6
5	T.Mulfunction-Functions-From-ECU	third party maintenance factory staff	normal operation/ use / maintenance maintenance	intentionally	For asset functions of VMG, it uses reverse engineering of the same product as the ECU firmware connected to CAN1-5, update ECU firmware connected to CAN1-5 to an unauthorized firmware, in this way, sends unauthorized data from ECU connected to CAN1-5, causes a malfunction of this functionality	5.6
6	T.DoS-Functions-From-Mobile-Device	third party	normal operation/ use / maintenance	intentionally	For asset functions of VMG, it impersonates a server, sends a huge amount of data from mobile connection device, interferes this functionality	9.4

1st Reason of Increase in Darknet Traffic



Unique number of hosts / day

TCP 宛先ポート別ホスト数 Top 10

宛先ポート	ホスト数	割合
23	71,981	78%
3389	8,999	10%
445	1,913	2%
	1,884	

Total number of Packets / day

TCP 宛先ポート別パケット数 Top 10

宛先ポート	パケット数	割合
23	4,266,598	54%
22	366,614	5%
8080	266,535	3%
	181,259	

National Institute of Information and Communications Technology

Type of Messages

Type	Subtype	From	To	Purpose
diagnose	request	VMG	ECU	Request of diagnose of software status
	report	ECU	VMG	Result of diagnose including software status
	submit	VMG	Usvr	Report of results of ECUs in a vehicle
	receipt	Usvr	VMG	Receipt for submit of diagnose report
update_check	request	VMG	Usvr	Request of update module
	response	Usvr	VMG	Update module is provided
update	notification	VMG	U/I	Notification message to introduce update for the driver
	confirmation	U/I	VMG	Confirmation message from the driver to apply update
	application	VMG	ECU	Request message including update module
	result	ECU	VMG	Result of application of the update module
update_report	submit	VMG	Usvr	Report of application of the update
	receipt	Usvr	VMG	Receipt of the report

* Usvr: Update server

* U/I: User Interface

National Institute of Information and Communications Technology