# Secure software updates for ITS communications devices

– International Standardization Activity in ITU-T SG17 –

Masashi Eto,
Senior researcher, Cybersecurity laboratory,
Network security research institute, NICT

# Outline

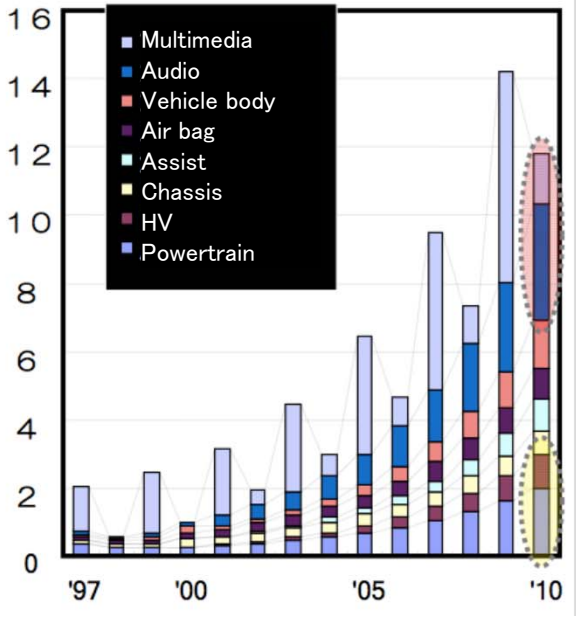
- Background
  - Computerization of vehicle
  - Necessity of remote update (maintenance) of vehicle
  - Threats against networked vehicle
- General remote update procedure and threat analysis
- An approach of international standardization in ITU-T
  - Introduction of "Secure software update capability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

# Background

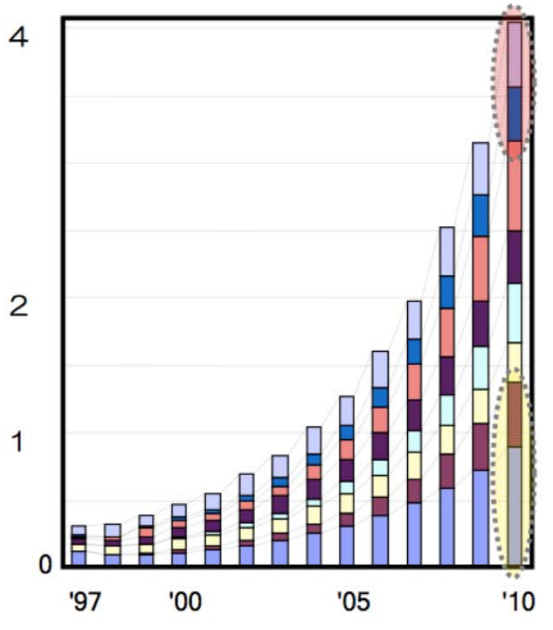
# Computerization of vehicle

| 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



Network Incident Analysis Center for Tactical Emergency Response

# 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.

- Manufacturers and users expect benefit from the remote update service

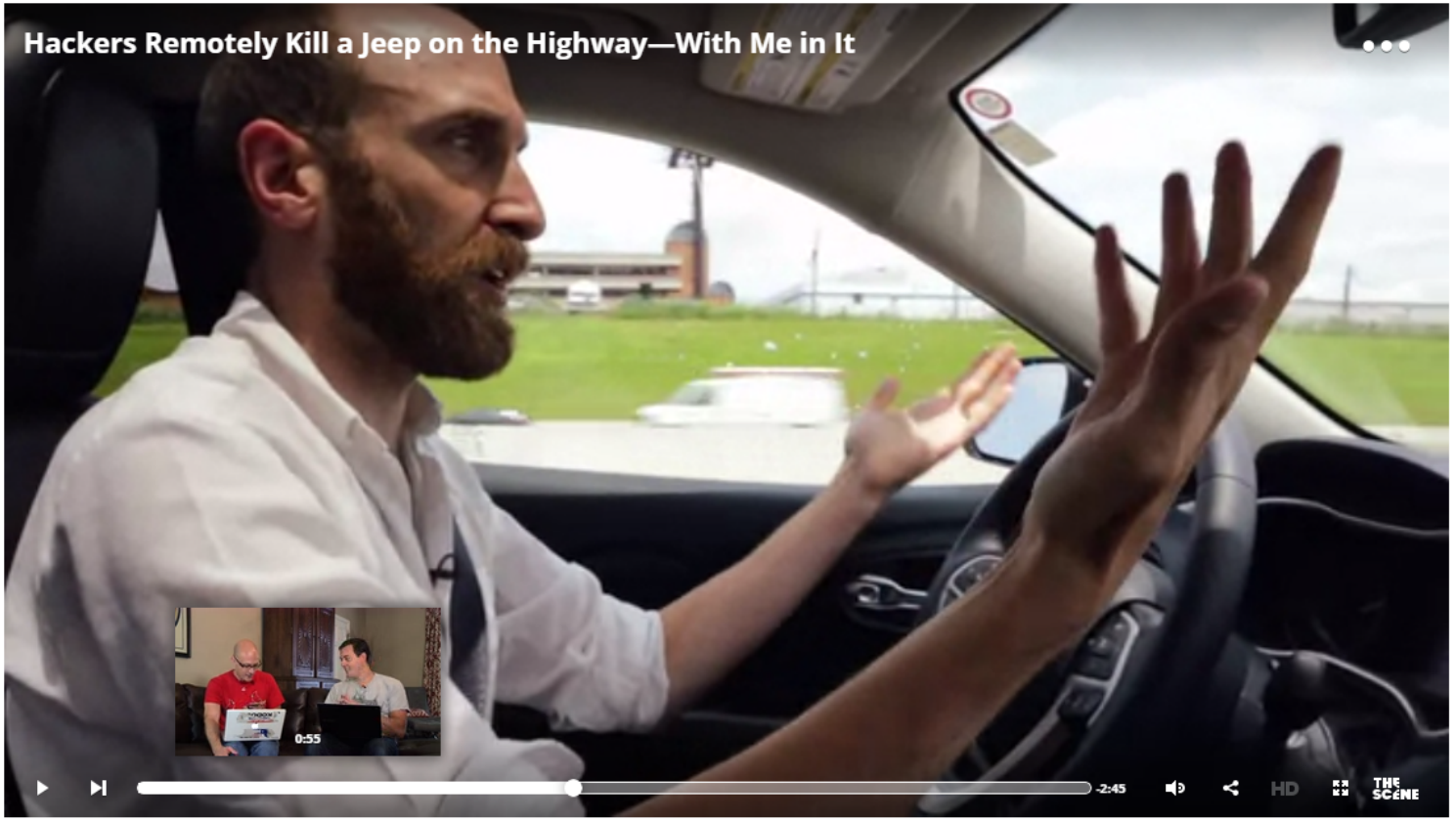
# Remote exploitation against FIAT Chrysler's Jeep Cherokee

WIRED Hackers Remotely Kill a Jeep on the Highway—With Me in It

BUSINESS | DESIGN | ENTERTAINMENT | GEAR | SCIENCE | SECURITY

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

## HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT






ident
nter
Response

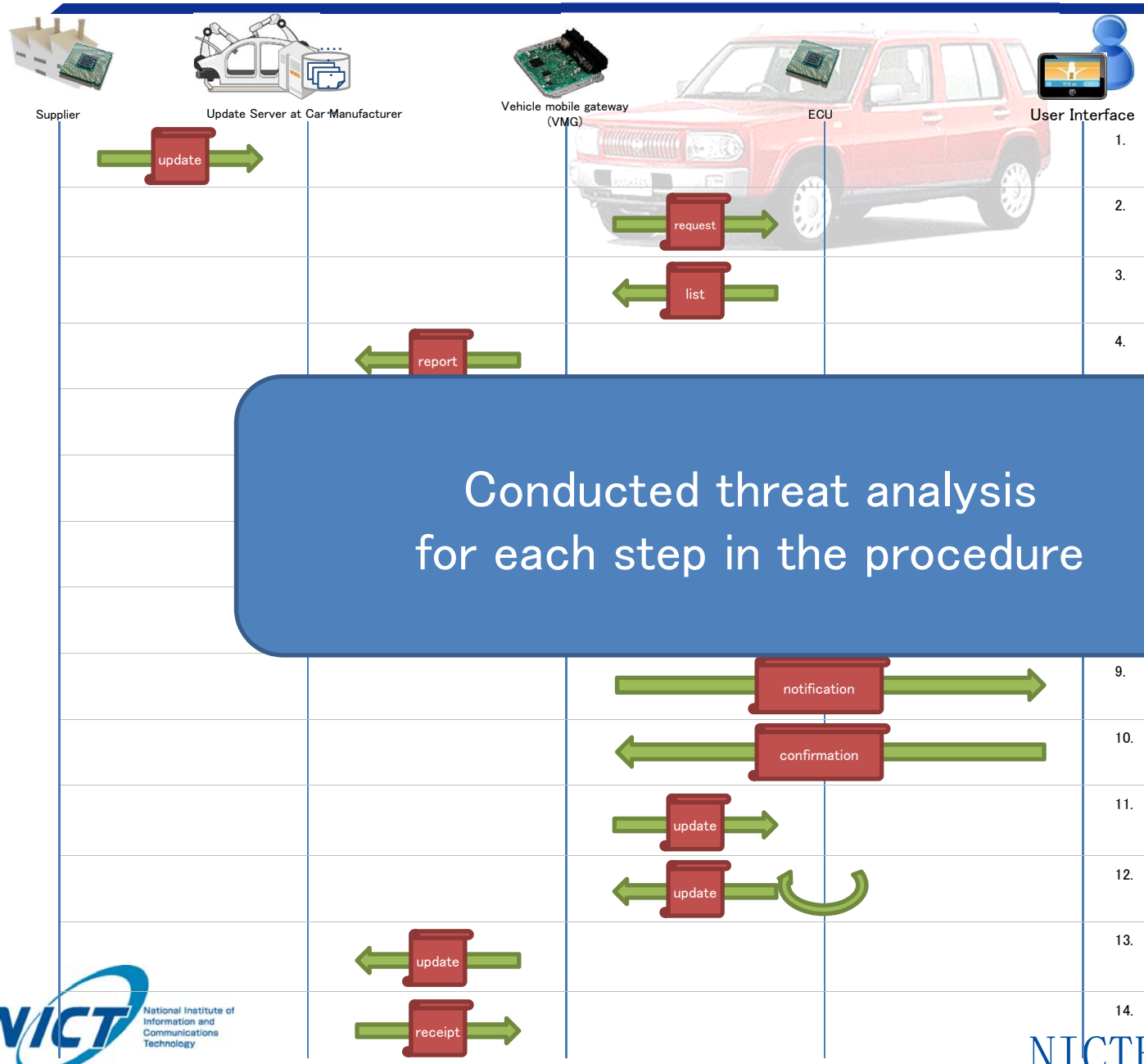
# Remote exploitation against FIAT Chrysler's Jeep Cherokee

- Research activity by two hackers
  - An article published in a news website
  - Detail will be 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 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

# General remote update procedure and threat analysis for networked vehicle

# Model data flow of remote software update




Conducted threat analysis
for each step in the procedure

1. Supplier provides an update module to a car manufacturer.
2. Vehicle mobile gateway requests ECUs to diagnose themselves and submit their software list.
3. ECUs generate a software list and submit it to the Vehicle mobile gateway.
4. The vehicle mobile gateway gathers the lists of software and submit them to update server.

ssues a receipt of the software list for ateway.

etermines necessary software modules

eriod of time, the vehicle mobile s update modules for the vehicle.

modules are delivered to vehicle

9. The gateway pushes a notification to a user interface.
10. The car owner confirms to apply the update via the user interface.
11. Vehicle mobile gateway delivers the updates to corresponding ECUs and request them to apply the updates.
12. Each ECU applies the update and reports the application result to the vehicle mobile gateway.
13. Finally the vehicle mobile gateway submits a report of application results to the update server.
14. Finally the vehicle mobile gateway submits a report of application results to the update server.

# Threat analysis: example case 1



2. Vehicle mobile gateway requests ECUs to diagnose themselves and submit their software list.

**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

# Threat analysis: example case 2


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

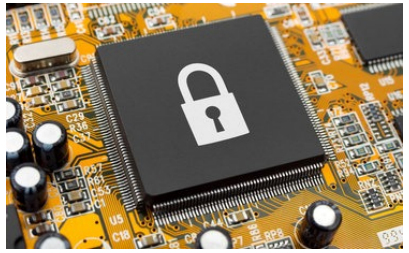
**Tampering / eavesdropping / replay of a message**

- 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)

# Functional Requirements for the secure 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.

# An approach of international standardization in ITU-T

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

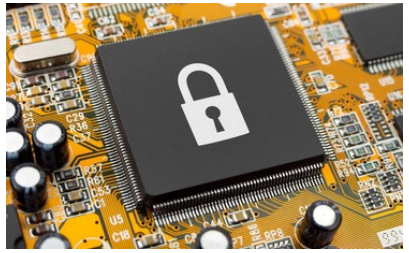
# Development of an ITU-T Recommendation

- 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
- Editor
  - Masashi Eto (NICT)
  - Koji Nakao (KDDI/NICT)

# Functional Requirements for the secure 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

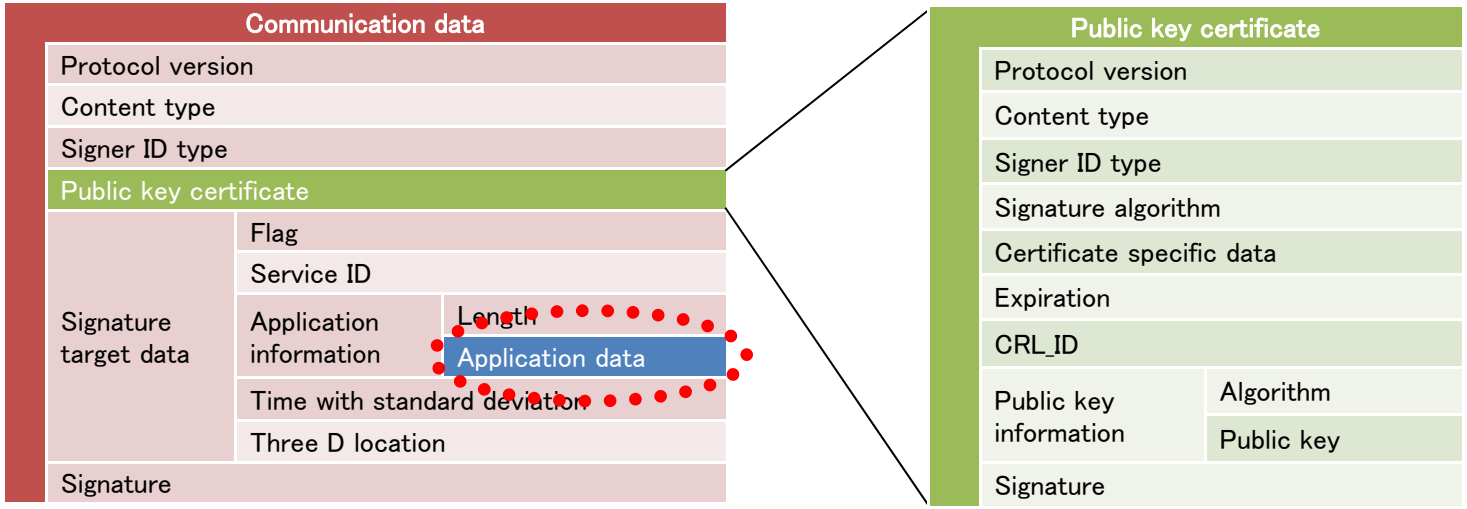


- ✓ Authentication of communication entity
  - Threats: impersonation of the entities
  - Measure : authentication of both client and server of each communication based authentication protocol such as SSL/TLS

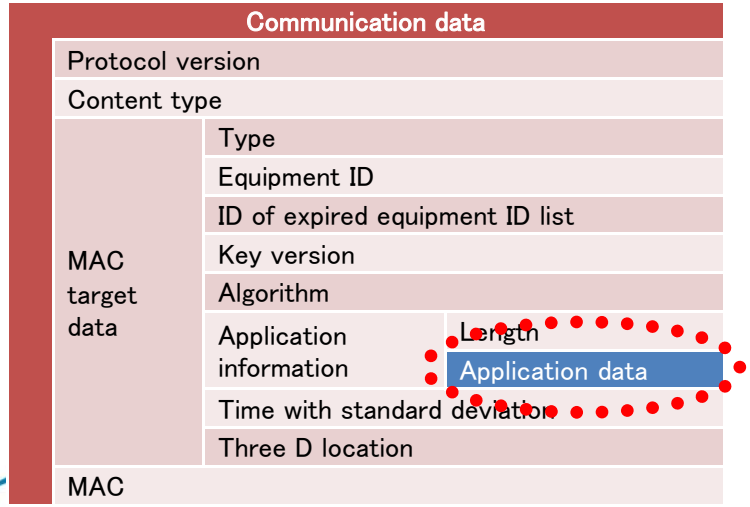
- ✓ Message filtering
  - Threats: DoS attack against VMG or update server
  - Measure : message filtering based on white listing of senders and frequency limitation of received messages, etc.

# General message format with security functions

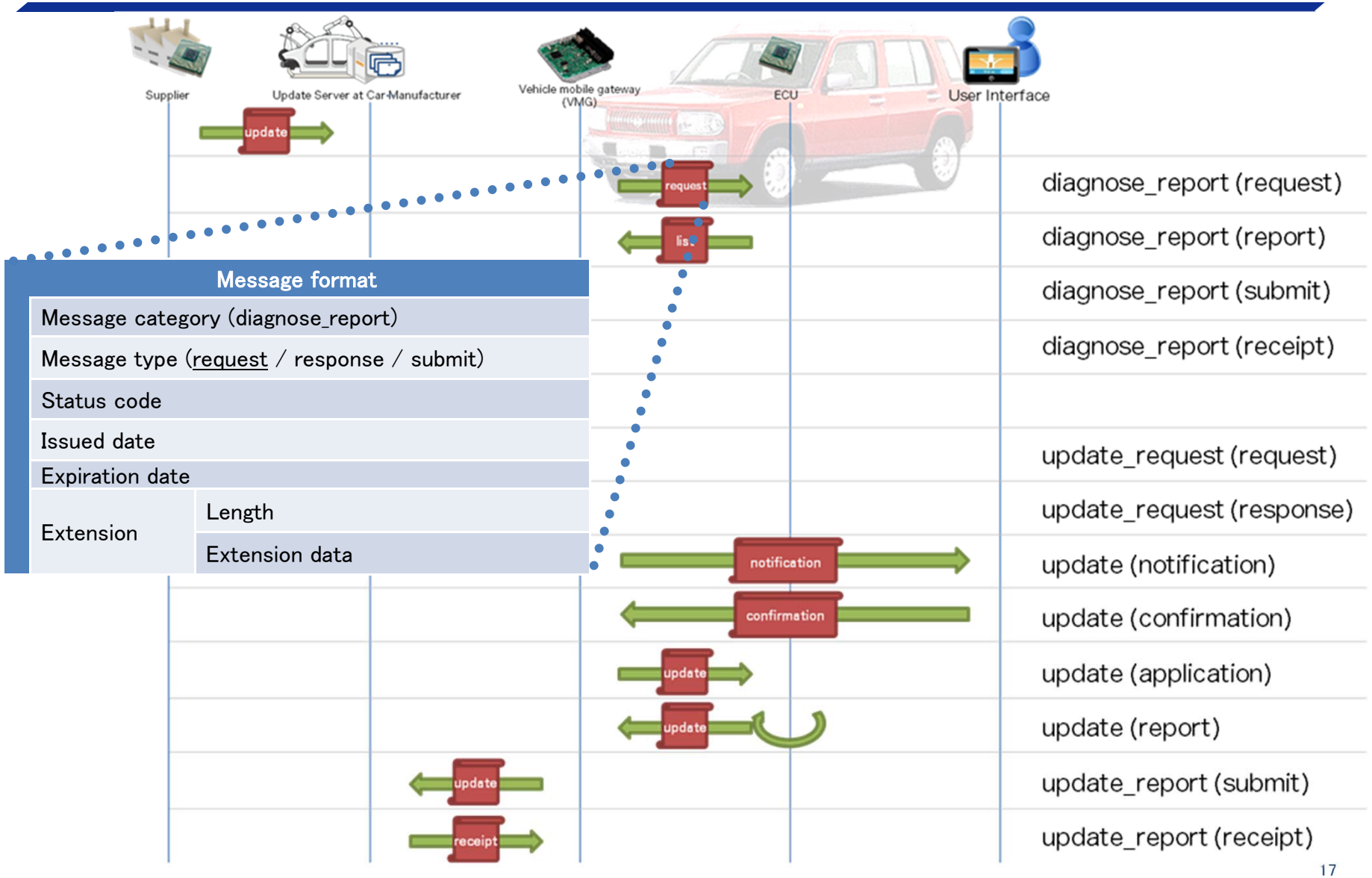
- Digital signature method message




- MAC method message



# Application data format for each message type




| Message format | |
|---|---|
| Message category (diagnose_report) | |
| Message type (request / response / submit) | |
| Status code | |
| Issued date | |
| Expiration date | |
| Extension | Length |
| | Extension data |

# 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"
    - Message verification
    - Trusted boot
    - Authentication of communication entity
    - Message filtering
  - **The standardization activity on this topic should be accelerated in corporation with car manufactures/venders in ITU-T SG17**
- Future plan for developing this Recommendation
  - ITU-T SG17 meeting at Geneva, Sep, 2015
    - Pre-final revision to request for comments
  - ITU-T SG17 meeting at Geneva, Mar, 2016
    - To be approved as a Recommendation

# Threat analysis

- In total, 53 threats have been found.
- According to the threats, possible countermeasures have been studied.

ITU－Tで53の脅威解析を実施していないと思いますが、どこのを引用していますか？？

| Step # | Step | Instance | Threat | Threat ID | Category of threat | Countermeasure |
|---|---|---|---|---|---|---|
| 1 | Supplier provides an update module to a car manufacturer. | Supplier | Improper update module is delivered to the update server | T.1-1 | Impersonation | authentication |
| | | Communication Path | Improper update module is delivered to the update server by an attacker on the path | T.1-2 | Tampering / eavesdropping / replaying | verification of message |
| | | | Latest update module is improperly acquired | T.1-3 | Impersonation | |
| | | | DoS attack against the update server by sending forged data (e.g., enormously huge data) | T.1-4 | DoS | Message filtering |
| | | Update Server | Latest update module is improperly acquired by an attacker | T.1-5 | Impersonation | |
| 2 | Vehicle mobile gateway requests ECUs to submit their software list. | VMG | Software information on every ECU in the vehicle is improperly acquired | T.2-1 | Impersonation | |
| | | Communication Path | Improper software information is uploaded to VMG | T.2-2 | Tampering / eavesdropping / replaying | |
| | | | Software information on every ECU in the vehicle is eavesdropped | T.2-3 | Tampering / eavesdropping / replaying | |
| | | | DoS attack against VMG by sending forged data (e.g., enormously huge data) | T.2-4 | DoS | |
| | | ECU | Improper software information is uploaded to VMG | T.2-5 | Impersonation | |
| | | | DoS attack against VMG by sending forged data (e.g., enormously huge data) | T.2-6 | DoS | |
| 3 | ECUs send Vehicle mobile gateway diagnoses an ECU to generate a software list. | VMG | Software information on every ECU in the vehicle is improperly acquired | T.3-1 | Impersonation | |
| | | Communication Path | Improper software information is uploaded to VMG | T.3-2 | Tampering / eavesdropping / replaying | |
| | | | Software information on every ECU in the vehicle is eavesdropped | T.3-3 | Tampering / eavesdropping / replaying | |
| | | | DoS attack against VMG by sending forged data (e.g., enormously huge data) | T.3-4 | DoS | |
| | | ECU | Improper software information is uploaded to VMG | T.3-5 | Impersonation | |
| | | | DoS attack against VMG by sending forged data (e.g., enormously huge data) | T.3-6 | DoS | |
| 4 | The vehicle mobile gateway uploads the lists of software modules to update server. | Update Server | Software information in the vehicle is improperly acquired | T.4-1 | Impersonation | |
| | | Communication Path | Improper software information is uploaded to the update server by an attacker on the path | T.4-2 | Tampering / eavesdropping / replaying | |
| | | | Software information in the vehicle is eavesdropped | T.4-3 | Tampering / eavesdropping / replaying | |
| | | | DoS attack against the update server by sending forged data (e.g., | T.4-4 | DoS | |

# Remote exploitation against Jeep Cherokee

WIRED Hackers Remotely Kill a Jeep on the Highway—With Me in It

BUSINESS DESIGN ENTERTAINMENT GEAR SCIENCE SECURITY

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

## HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

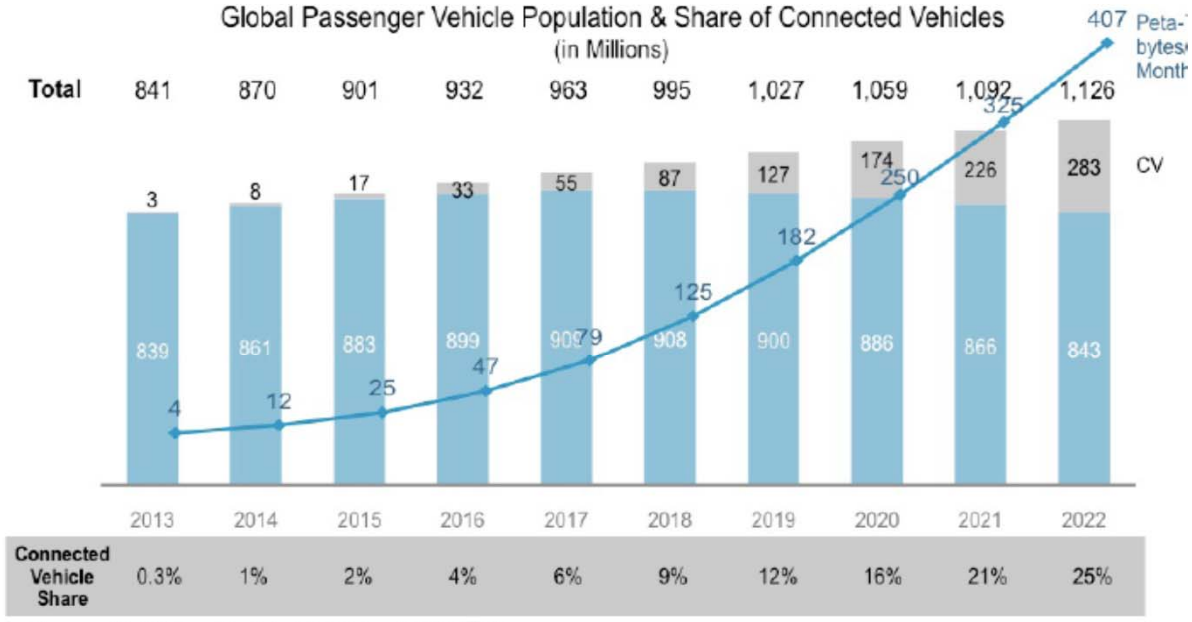


ident
nter
Response

# 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

# Scope of the Recommendation

**Functionality of Server**

- Stored Data Definition
  - ✓ Auth info
  - ✓ Log Audit
  - ✓ With considerations of privacy concerns

**Communication protocol**

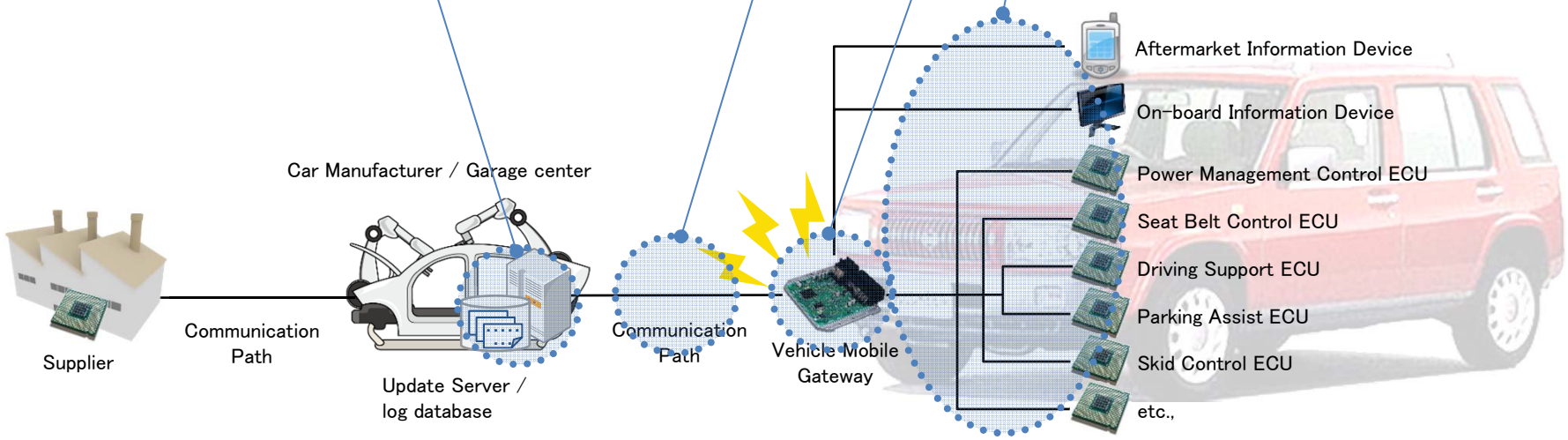
- Between Car and Manufacturer / Garage
- Encryption
- Authentication

**Functionality of Head Unit**

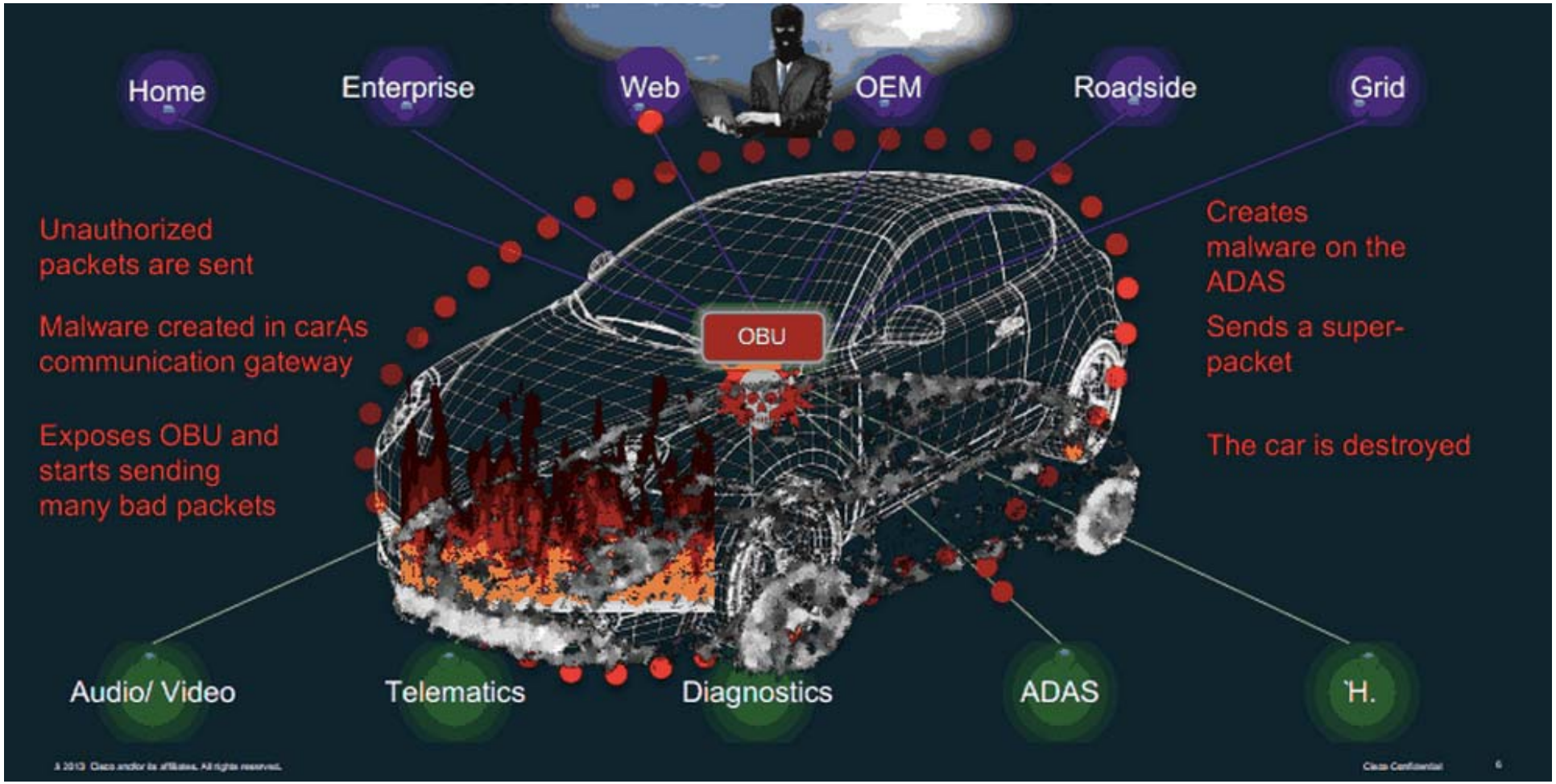
- Status check of ECUs
- Log collection
- In-car diagnosis function

**Diagnosis of on-board devices**

- Status check of ECUs
- Log collection
- Verification of update module



# More Attacks Surfaces!




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

# General model of networked vehicle