Introduction of ITU-T Study Group 17
Standardization of “Security”

Koji Nakao
NICT, Japan
WP chair of ITU-T SG17

SG17 Responsibility & mandates

WTSA-16 approved the role of SG17:

- **ITU–T Study Group 17 – Security (Chairman: Prof. Heung Youl YOUM/Korea (Republic of))**

- ITU–T Study Group 17 is responsible for building confidence and security in the use of information and communication technologies (ICT). This includes studies relating to cybersecurity, security management, countering spam and identity management. It also includes security architecture and framework, protection of personally identifiable information, and security of applications and services for the Internet of things (IoT), smart grid, smartphone, software-defined networking (SDN), Internet Protocol television (IPTV), web services, social network, cloud computing, big data analytics, mobile financial system and telebiometrics.
- Study Group 17 is also responsible for the application of open system communications, including directory and object identifiers, and for technical languages, the method for their usage and other issues related to the software aspects of telecommunication systems, and test specification languages in support of conformance testing to improve the quality of Recommendations.

ITU-T Study Group 17
Security

ITU-T Study Group 17 Questions

- WTSA-16 confirmed the 12 Questions of SG17:

Question number	Question title	Status
1/17	Telecommunication/ICT security coordination	Continuation of Q1/17
2/17	Security architecture and framework	Continuation of Q2/17
3/17	Telecommunication information security management	Continuation of Q3/17
4/17	Cybersecurity	Continuation of Q4/17
5/17	Countering spam by technical means	Continuation of Q5/17
6/17	Security aspects of telecommunication services and networks	Continuation of Q6/17
7/17	Secure application services	Continuation of Q7/17
8/17	Cloud computing security	Continuation of Q8/17
9/17	Telebiometrics	Continuation of Q9/17
10/17	Identity management architecture and mechanisms	Continuation of Q10/17
11/17	Generic technologies (Directory, Public-Key Infrastructure (PKI), Privilege Management Infrastructure (PMI), Abstract Syntax Notation 1 (ASN.1), Object Identifiers (OIDs)) to support secure applications	Continuation of Q11/17
12/17	Formal languages for telecommunication software and testing	Continuation of Q12/17

ITU-T Study Group 17
Security

Security Areas covered by SG17

- Cybersecurity – Cybex
- Countering spam
- Information Security Management
- Fundamental security: PKI, X.509…
- Identity Management (IdM)
- Application security

Covered by Q6/17

- ✓ Home network, IoT, ITS, smart grid, smartphone, SDN, IPTV, web services, etc.
- ✓ Cloud computing, big data analytics, and telebiometrics.

Approach taken by SG17 for developing security standards (6 steps)

1. **High level requirement : kick-off to study**
2. **Reference Model**
   The reference model should be identified for security considerations;
3. **Threats analysis**
   Based on the model, threats should be identified and analyzed;
4. **Risk Assessment**
   Based on the threats, risk should be assessed and identified;
5. **Security Requirements**
   Based on the risk assessment, security requirements should be developed;
6. **Security Controls**
   Based on the requirements, security controls (countermeasures) should be identified and implemented.

To seek out “high level security Requirement”, NICT research activities may be helpful…

Cyber attacks in IoT on the rise

Thingbots: The Future of Botnets in the Internet of Things

February 20, 2016 | By Paul Sabanal

The Internet of Things (IoT
upon us. Everything from
home appliances, watches
even children's toys are be
connected online. It is proj
that by the year 2020, ther
be more 25 billion devices

Home Router Botnet Leveraged in
Large DDoS Attack

Is your refrigerator really part of a massive spam-sending botnet?

Ars unravels the report that hackers have commandeered 100,000 smart devices

by Dan Goodin - Jan 18, 2014 5:25am JST

Internet of Things security concerns boost in IoT services

by

News roundup: As Internet of Things concerns rise reality, one vendor is quick to ...to combat the risks. Plus: 1% of use...e risk; Target pays up; Apple devic...ly secured in the enterprise.

RISK ASSESSMENT / SECURITY & HACKTIVISM

"Internet of Things" is the new Windows XP —malware's favorite target

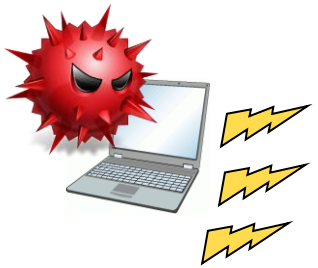
Two approaches to monitor attacks

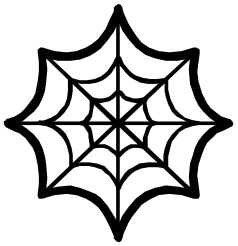
- **Passive monitoring**
  Prepare network to monitor attacks and wait
  - Darknet monitoring
  - Honeypot

- **Active monitoring**
  Search for device/vulnerability/backdoors
  - Accessing Web, Telnet, FTP, etc to decide what devices they are
  - Checking for backdoor ports
  - Measuring clock skew for tracing individual devices

Darknet monitoring

Darknet: unused but routable IP address (es) or net blocks





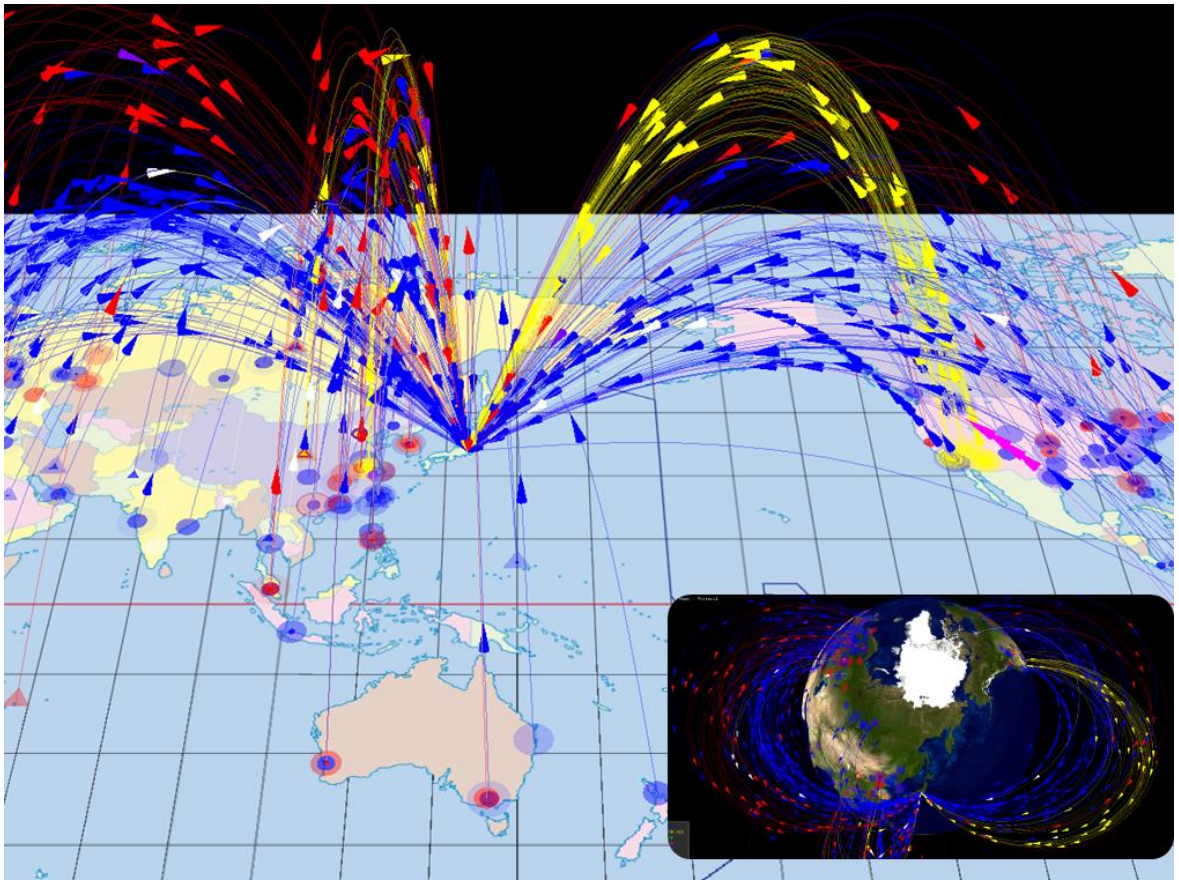
Many researchers/organization utilize darknet to monitor malicious activities like scanning, remote exploits, back scatters, etc

Scanning observation by nicter-Atlas

Recently, “scanning to Port 23 (telenet)” is getting larger!!

- Capturing packets through dark-net in real time basis.
- Color indicates the protocol types.

UDP
TCP SYN
TCP SYN/ACK
TCP Other
ICMP



Increases of telnet attacks

packets

7
6
5
4
3
2
1

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	2,699,639	45%
22	461,738	8%
80	348,077	6%
1433	208,460	3%
3306	199,372	3%
3389	151,868	3%
8080	145,657	2%
443	124,800	2%
9200	116,255	2%
25	94,901	2%

1/1/2005 1/1/2006 1/1/2007 1/1/2008 1/1/2009

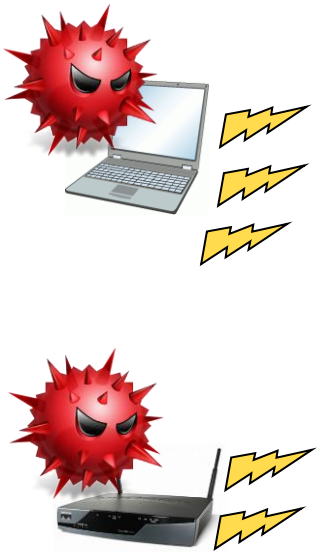
TCP 宛先ポート別パケット数 Top 10

宛先ポート	パケット数	割合
23	11,727,894	65%
1433	791,485	4%
22	559,059	3%
3389	247,547	1%
80	247,159	1%
8080	184,132	1%
443	147,434	1%
3306	128,382	1%
4028	116,029	1%
54628	78,378	0%

10 years observation of NICTER darknet (23/tcp only)

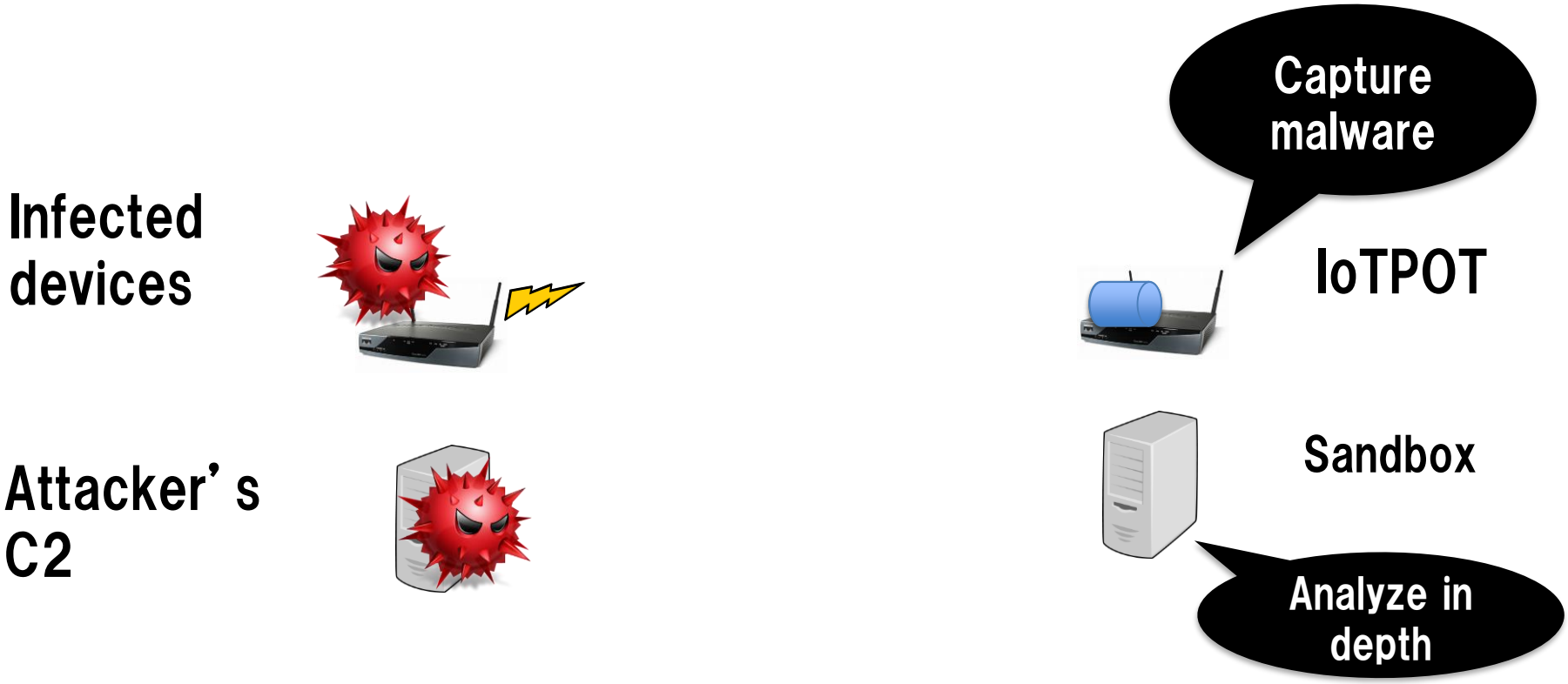
To monitor in depth

Darknet monitoring is simple and great to monitor wider networks but limited as it only gets the first packet of each attack.



Our system: IoTPOT = IoT Honeypot

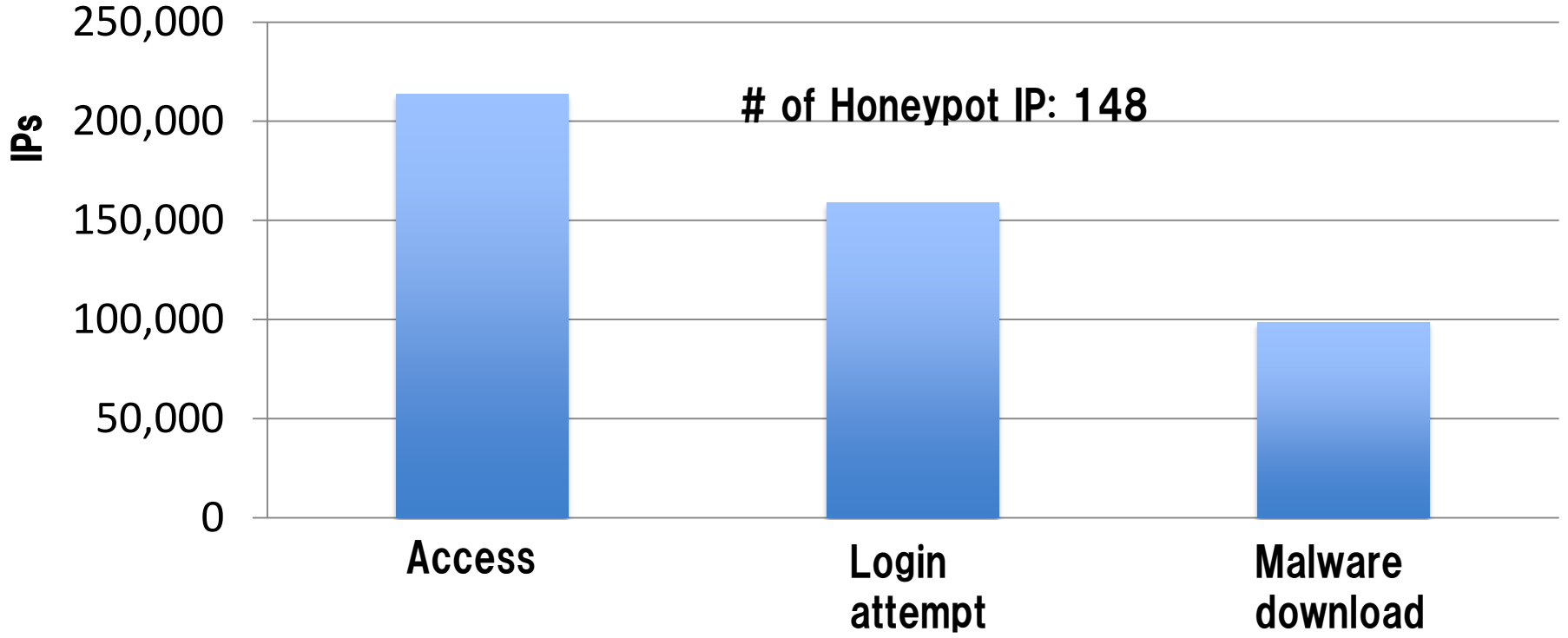
We use decoy system (honeypot) to emulate vulnerable IoT devices to monitor the attacks in depth



Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," USENIX WOOT 2015

Observation result (last year)

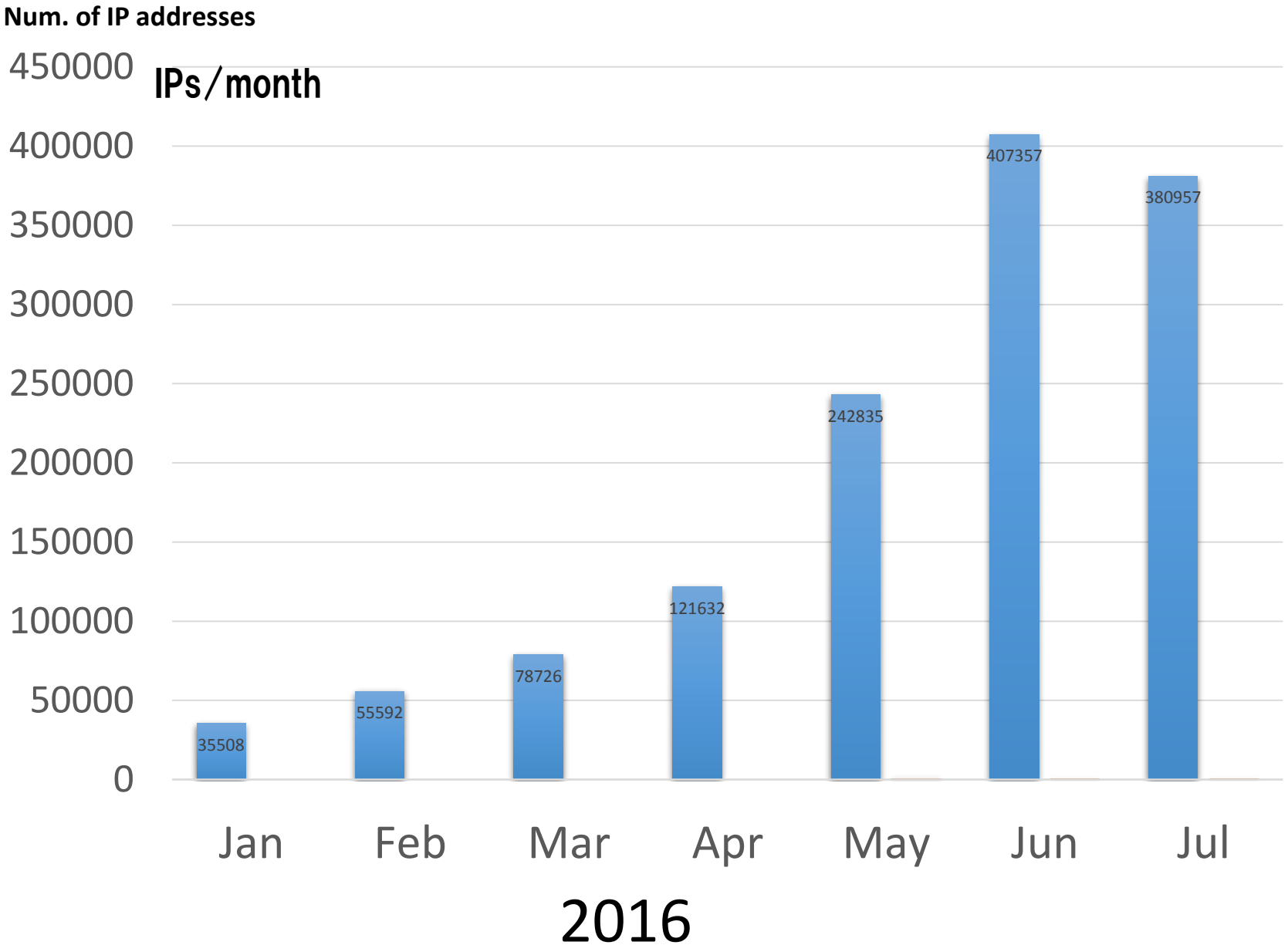
Period:2015/4/1～2015/7/31 (122days)



150,000 IPs attempted to login, 100,000 actually did send us malware binaries

Binaries with 11 different CPU architectures
93% of the binaries were new in VT (as of 2015/9/24)

Increase of attacks



Devices attacked our honeypot during Jan-June 2016

Categories of Inferred Infected devices (2016.9)

- Surveillance camera
  - IP camera
  - DVR
- Network devices
  - Router, Gateway
  - Modem, bridges
  - WIFI routers
  - Network mobile storage
  - Security appliances
- Telephone
  - VoIP Gateways
  - IP Phone
  - GSM Routers
  - Analog phone adapters
- Infrastructures
  - Parking management system
  - LED display controller



Devices are inferred by telnet/web banners

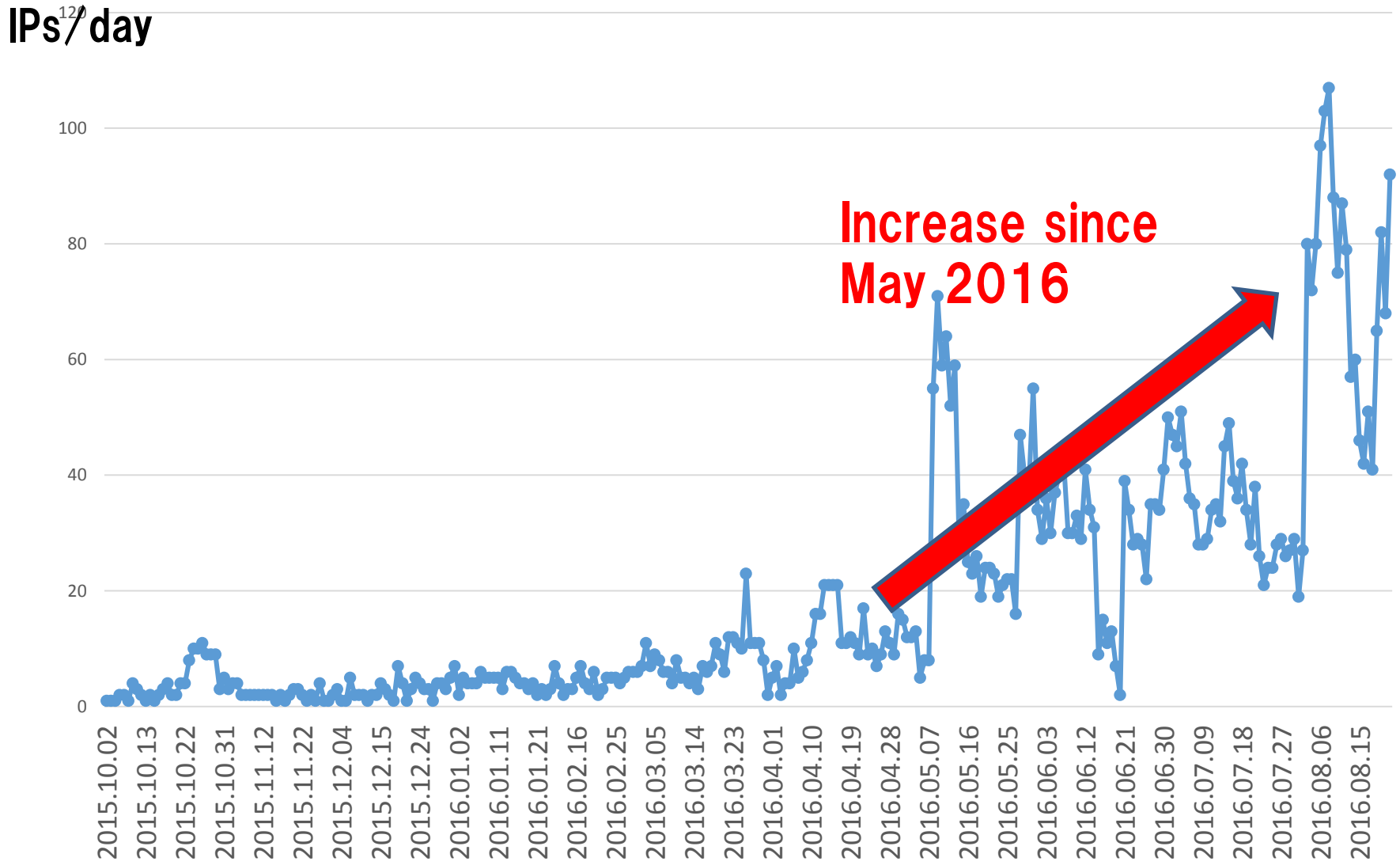
- Control system
  - Solid state recorder
  - Sensors
  - Building control system (bacnet)

Home/indivisuals

- Web cam, Video recorders
- Home automation GW
- Solar Energy Control System
- Energy demand monitoring system

- Broadcasting
  - Media broadcasting
  - Digital voice recorder
  - Video codec
  - Set-top-box,
- Etc
  - Heat pump
  - Fire alert system
  - Medical device (MRI)
  - Fingerprint scanner

Infected devices in Japan (Daily count)



IoT Devices are attacked and scanned

Wireless Router

Food Processing Machine

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

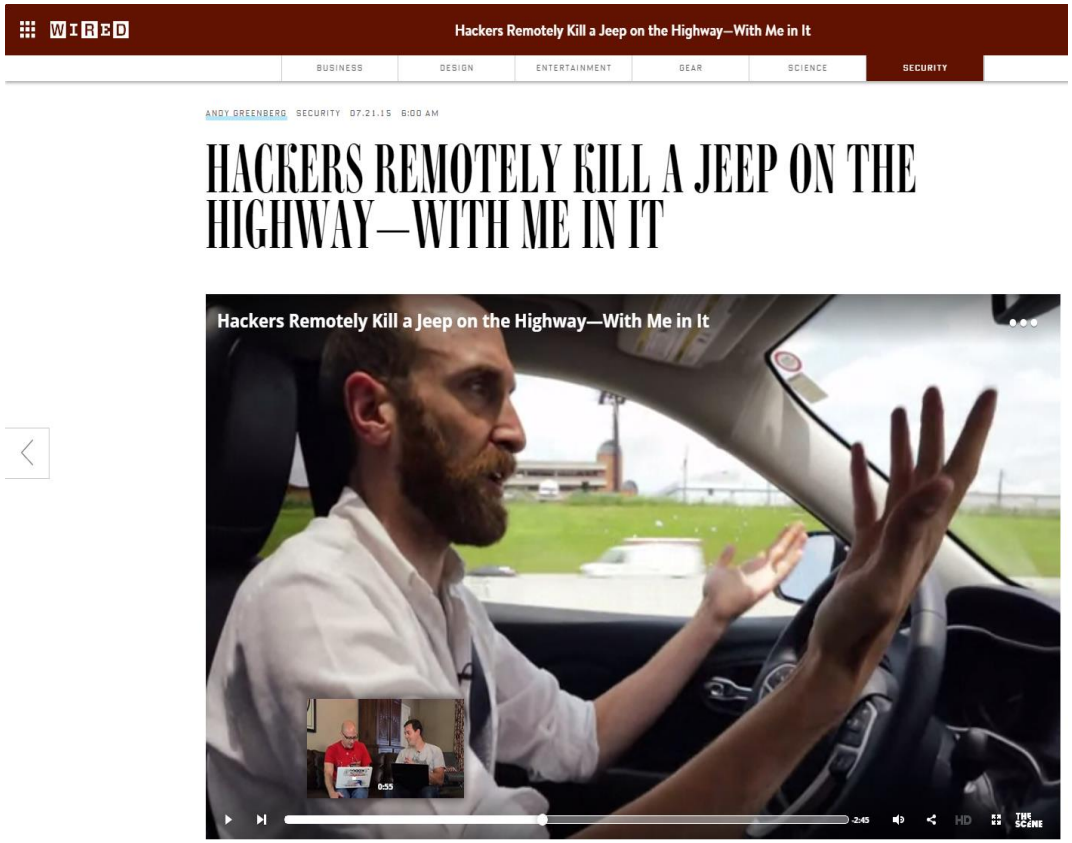
Heat Pump

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 exploit attack was conducted 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

National Institute of Information and Communications Technology

High level Requirement for “remote update (maintenance) of vehicle”

- **Improvement of vehicle**
  - **Against remote exploitation and so on, Software modules inside Vehicle 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 may expect benefit from the remote update service in secure manner**

NICT National Institute of Information and Communications Technology

Draft Recommendation ITU-T X.1373 (X.itssec-1)

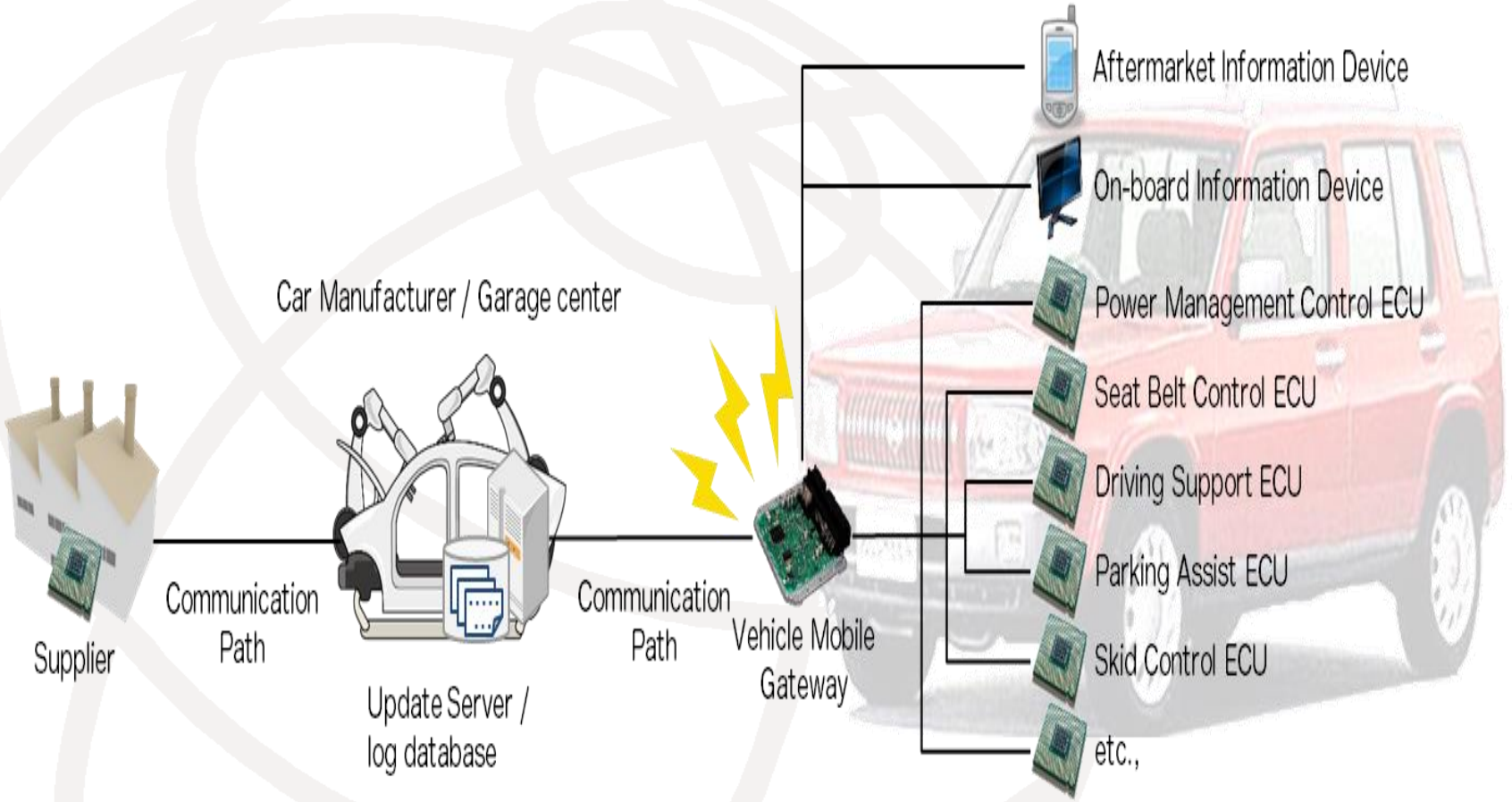
- **Secure software update capability for intelligent transportation system communications devices**

- **Scope (initial) :**
  - In the context of updates of software modules in the electric devices of vehicles in the intelligent transportation system (ITS) communication environment, **this Recommendation aims to provide a procedure of secure software updating for ITS communication devices for the application layer.** This includes a basic model of software update, its threat and risk analysis, security requirements and controls for software update and a specification of abstract data format of update software module.

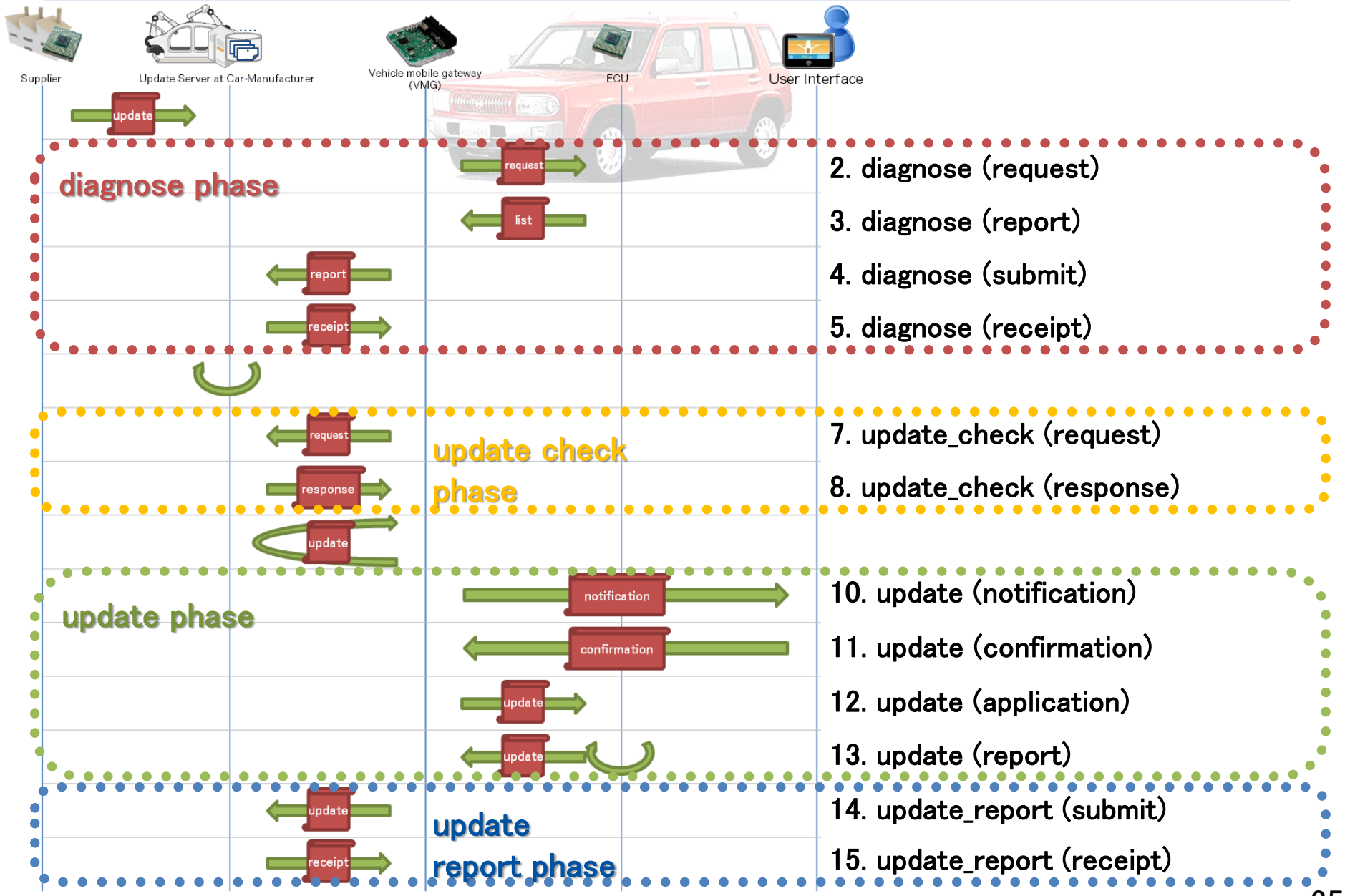
In the case of Rec. X.itssec-1, the following approach was taken

1. **High level security requirement**
   Software updates for Vehicle should be securely conducted;
2. **Reference Model**
   The reference model is simply designed only for software updates;
3. **Threats analysis**
   Did only for the software updates based on the model;
4. **Risk Assessment**
   Skipped to conduct risk assessment and impact analysis. This is superseded by the threats analysis;
5. **Security Requirements**
   Did identify the requirements based on the threats analysis;
6. **Security Controls**
   Did specify the secure procedure for software updates between Vehicle and Update server.

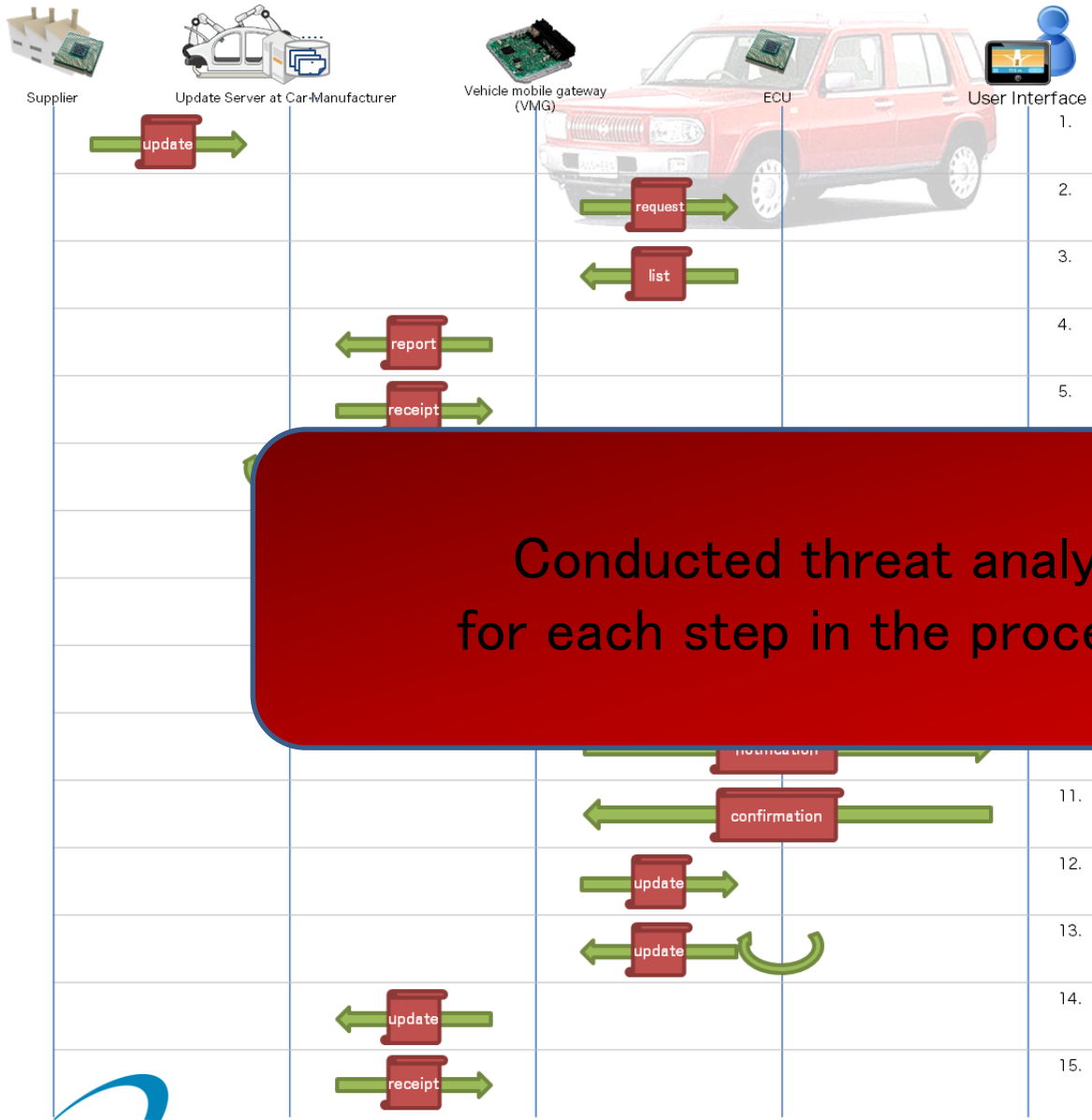
Reference Model (initial)



Protocol/Procedure based on the reference model



Threats Analysis was conducted



1.
2. Request of diagnose of software status
3. Result of diagnose with software status
4. Report of results of ECUs in a vehicle
5. Receipt for submit of diagnose report

Conducted threat analysis
for each step in the procedure

11. Confirmation for the update
12. Request for updates to ECUs
13. Results for updates in ECUs
14. Report of application of the update
15. Conformation from the Update server

National Institute of Information and Communications Technology

Threat analysis: Procedure 2 (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: Procedure 2 (1)

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

National Institute of Information and Communications Technology

Threat analysis: Procedure 3 (1)

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)

Threat analysis: Procedure 3 (2)

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

National Institute of Information and Communications Technology

Threat analysis: Procedure 4 (1)

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., enormously huge data)	T.4-4	DoS
		VMG	Improper software information is uploaded to the update server	T.4-5	Impersonation
			DoS attack against the update server by sending forged data (e.g., enormously huge data)	T.4-6	DoS

National Institute of Information and Communications Technology

Security requirements and Controls (Measures)

- ✓ **Message used in the software update shall be verified**
  - Threats: tampering, eavesdropping and replaying of messages
  - Control: message verification mechanism based on Message Authentication Code (MAC) or digital signature method

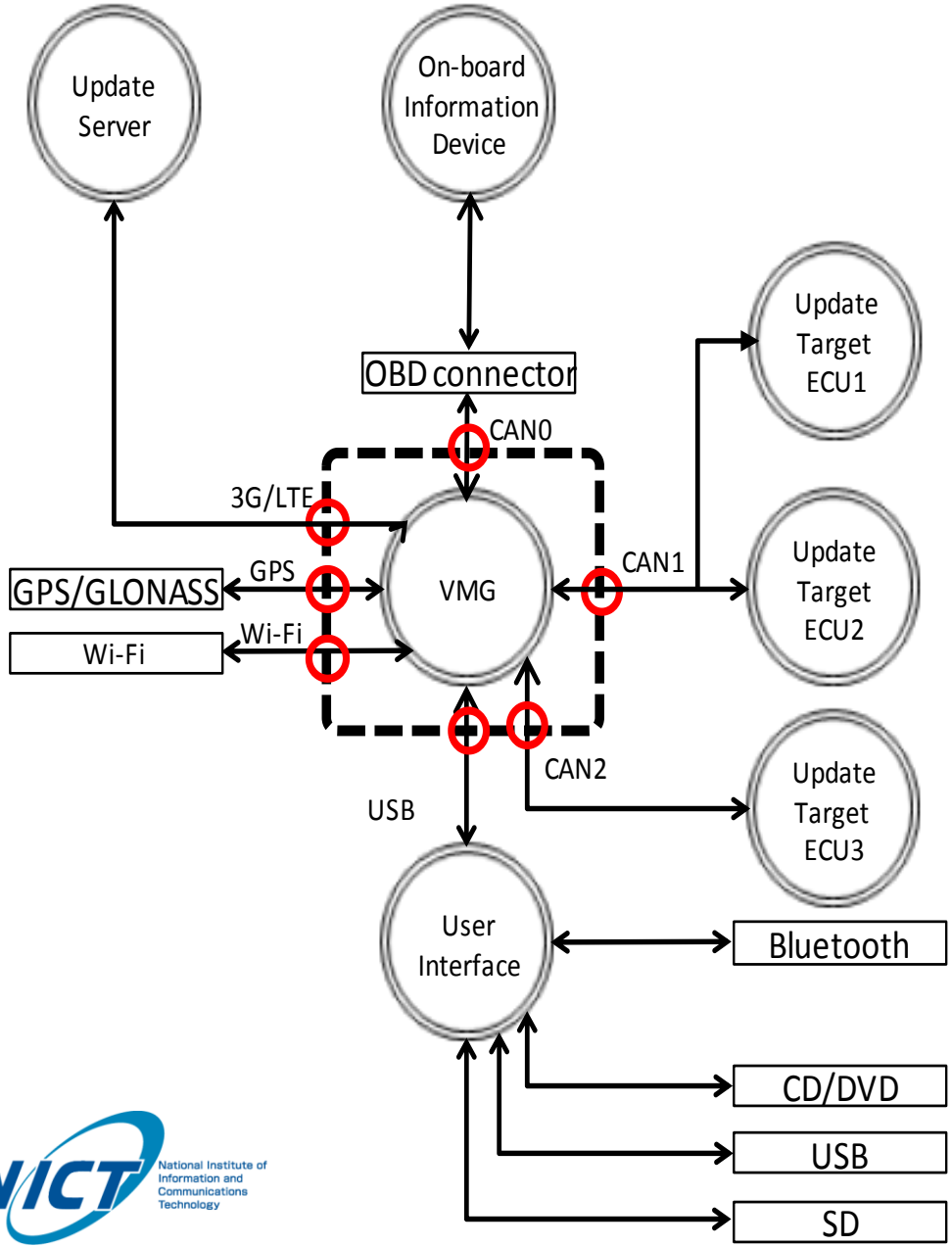
- ✓ **Trusted boot of ECUs shall be equipped**
  - Threats: tampering of software in ECU
  - Control : hardware Security Module (HSM) to verify software modules in ECUs' boot sequences

- ✓ **Communication entities shall be authenticated**
  - Threats: impersonation of the entities
  - Control : authentication of both client and server of each communication based authentication protocol such as SSL/TLS

- ✓ **Messages related to DoS attack shall be filtered out**
  - Threats: DoS attack against VMG or update server
  - Control : message filtering based on white listing of senders and frequency limitation of received messages, etc.

- ✓ **Fault tolerance shall be equipped against DoS attack**
  - Threats: DoS attack against VMG
  - Control : 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.

Analysis based on TOE (Target of Evaluation) model



Actually, we did conduct threats analysis, risk assessment and identification of security requirements based on the TOE model focusing on VMG (Vehicle Mobile Gateway).

However, we have finally decided **NOT** to put these studies in the normative part of the Recommendation, since it is considered as premature work.
These works are in the appendixes of X.itssec-1.

Draft Recommendation ITU-T X.1373 (X.itssec-1)

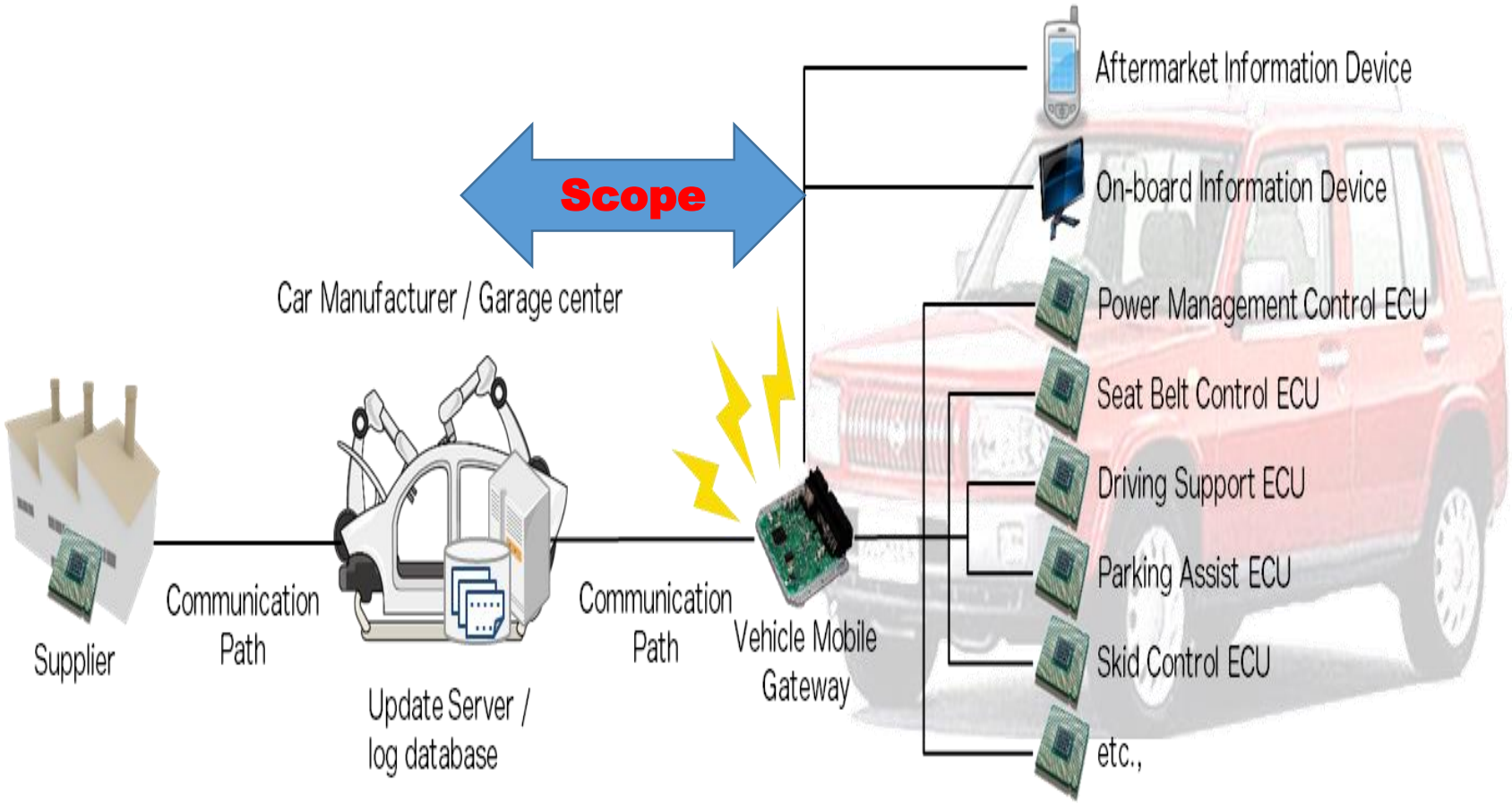
Secure software update capability for intelligent transportation system communications devices

(Status: 2016-09/ Determined (now in TAP consultation process))

Scope:

- In the context of updates of software modules in the electric devices of vehicles in the intelligent transportation system (ITS) communication environment, **this Recommendation aims to provide a procedure of secure software updating for ITS communication devices for the application layer in order to prevent threats such as tampering of and malicious intrusion to communication devices on vehicles. This includes a basic model of software update, security controls for software update and a specification of abstract data format of update software module.**
- **The procedure related to in-vehicle communication is the out of scope of this Recommendation. For reference, the procedure used in-vehicle in this Recommendation is informative.**
- The procedure is intended to be applied to communication devices on ITS vehicles under vehicle-to-infrastructure (V2I) communication by means of the Internet and/or ITS dedicated networks. The procedure can be practically utilized by car manufactures and ITS-related industries as a set of standard secure procedures and security controls.

Model for the software update in Draft Rec. ITU-T X.1373 (X.itssec-1) is reduced



The following issues are also considered to be in the Appendixes (informative) of the draft text of X.itssec-1.

Works conducted based on TOE focusing on VMG:

- Threat analysis
- Risk analysis
- Security Requirements
- Security Control

are in the Appendix I and II of X.itssec-1.

However, Security Controls related to Software updates are still in the normative text of X.itssec-1 as a set of security functions.

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION BUREAU

Geneva, 28 November 2016

Ref: **TSB Circular 246**
SG17/MEU

Tel: +41 22 730 5866

Fax: +41 22 730 5853

E-mail: tsbsg17@itu.int

To:

- Administrations of Member States of the Union

Copy to:

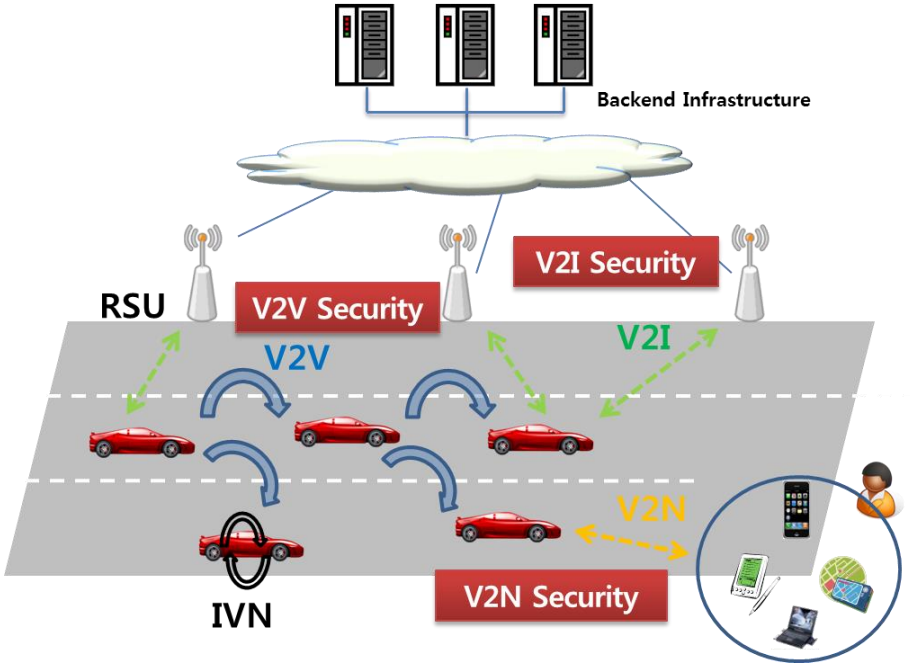
- ITU-T Sector Members;
- ITU-T Associates;
- ITU Academia;
- The Chairman and Vice-Chairmen of ITU-T Study Group 17;
- The Director of the Telecommunication Development Bureau;
- The Director of the Radiocommunication Bureau

Subject: **Meeting of ITU-T Study Group 17, 22-30 March 2017, Geneva, with a view to approving draft Recommendations ITU-T X.1 X.1126 (X.msec-11), X.1212 (X.cogent), X.136 X.1550 (X.nessa) in accordance with the prov WTSA (Rev. Dubai 2012)**

X.1373 (X.itssec-1)
Deadline: 13 March: Today

Draft Recommendation ITU-T X.itssec-2

- **Security guidelines for V2X communication systems**
  (Timing: 2017-10 / Determination)
  - Provides security guidelines for V2X communication systems. V2X means Vehicle-to-Vehicle (V2V), V2I (Vehicle-to-Infrastructure) and/or V2N (Vehicle-to-Nomadic Devices)
  - Includes analysis of threat and vulnerability for V2X communication systems
  - Provides the security requirements for V2X communication systems



Overview of the vehicular communication, in Draft Rec. ITU-T X.itssec-2

Content of X.itssec-2

This draft Recommendation will be actively discussed at the next SG17 meeting (March 22-30).

A Contribution from Korea (Hyundai Motors)

Title:

Proposal for a new Question on Security aspects for Intelligent Transport System

Rationales for a new Question on security aspects for ITS

- Having a new Question on security aspects for ITS in SG17 has following advantages:
- Attracting much more participation from global car makers;
- Accelerating to work on ITS security work (e.g., mechanisms and protocols for ITS security) in SG17 to meet the market needs;
- Providing clear visibility of ITS security work, inside and outside ITU;
- Providing a focal point for collaboration on ITS security with other relevant organizations; and
- Making a centre of competence of ITS security, within ITU and across the world.

Proposal

It is proposed to establish a new Question on security aspects for ITS under ITU-T SG17 with the proposed question text given in Annex A, and to delete text related to ITS work in the description of Question 6/17, in the case there is agreement to create the new Question.

Future works in SG17 on ITS

- Confirm the result of TAP consultation on X.itssec-1;
- Improve the draft Rec. X.itssec-2;
- Discuss for establishing a new question for ITS security;
- Collaboration with related SDOs on ITS;
- Roadmap of ITS security Recommendations to be developed in SG17 should be discussed and studied.

Collaboration with TFCS

- As for developing Rec. X.itsse-2 (Security Guideline for V2X communication systems), parts of threats analysis (assessment) can be shared and exchanged between TFCS and ITU-T SG17.
- Concerning X.itssec-1 (secure software update procedure), the Recommendation will be completed very soon in ITU-T SG17. This Recommendation is an initial study (baseline) and further improvement of “secure software update” is required based on this initial study. SG17 is expecting to improve this Recommendation collaboratively with TFCS.
- SG17 is still seeking out any valuable work items related to ITS security and expecting to receive input from TFCS (see OLs from CITS)

Additional Information on OTA

- In connection to X.itssec-1 (secure software update procedure), a technical report (TR) is going to be published in ITU-T SG16 (lead study group on ITS).
- Title of the TR is:
  Secure Over-the-Air Vehicle Software Updates
  - Operational and Functional Requirements -
- This TR can be referred from SG17 as a supporting document for X.itssec-1.

Thank you for listening