Risk Assessment Study on Threat cases of “Connected Car”

November 15, 2016
Connected Consumer Device Security Council (CCDS)
Managing Director / Secretary General
Kosuke Ito

Agenda

1. Brief Introduction of CCDS
2. Tendency of Threats on “Connected Car”
3. Risk Assessment of Threats on “Connected Car”
4. Summary

CCDS overview

- Name: General Incorporated Association - Connected Consumer Device Security Council
- Establishment: October 6, 2014
- Chairman: Hideyuki Tokuda (Professor of Keio University, Cabinet Security Advisor)
- Representative Director: Tsukasa Ogino (Specially Appointed Professor, Kyoto University)
- Managing Director: Kosuke Ito (Zero-one Laboratory)
- Directors: Atsuhiro Goto (Professor, Institute of Information Security, SIP: PD)
  Katsutoshi Hasegawa (President, eSOL Co., Ltd.)
  Hiroyuki Hattori (President, Witz Co., Ltd.)

- Number of members: 130 (as of the end of Sep, 2016)
  (Official members or higher: 44, General members: 62, Academic members: 14, Liaison members: 10)

- Main businesses:
  1. Internal/external trend investigation on security in various field of life devices, and interchange/cooperation with internal/external organizations
  2. Development of security technology which satisfies safety and security of life devices
  3. Development of security design process, development/preparation of verification method guidelines and promotion of international standardization
  4. Preparation/control of life device verification environment, verification business and human resource development on security, public relations/dissemination activity, etc.

Tendency of Threats on “Connected Car”

Example: JEEP hacking(BlackHat2015)

- Research which can remotely operate Jeep without physical modification
  - Interference with air conditioner, wiper, brake, transmission and steering. Automobile information can always be obtained.
  - Vulnerability:
    - Onboard WiFi was able to be viewed.
    - IP network on Sprint3G network was able to be viewed.
    - V850ECU firmware was replaced with a modified one.
  - 1.4 million recalls results in billion-yen scale damages.

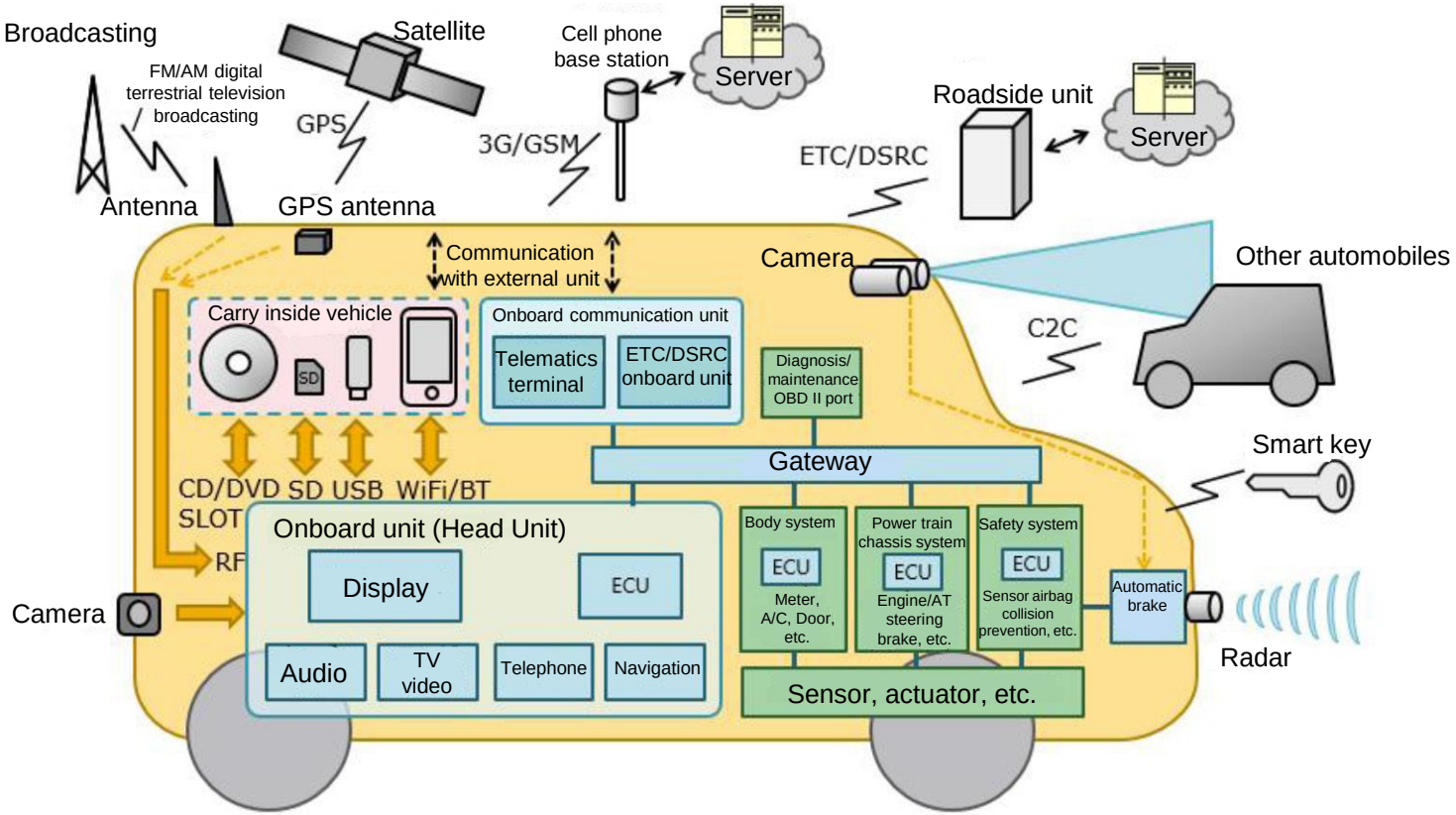
- Using vulnerability of Chrysler's connected car system "Uconnect"
  - Chip set firmware of the entertainment system is updated.
  - Interference with air conditioner, wiper, brake, transmission, steering.
  - Steering operation is taken during reverse movement.
  - Other vehicle information in the network can be obtained without update of the firmware.
    Automobile information can be taken.
- Chrysler takes the action by providing a patch.
  (Update by USB or maintenance shop)

Image: Uncontrolled brake results in ditch. (Source: IRED)

Reviewed system model

■ System model for review

Creation of the system model for review summarizes the automobile function. In analysis of the threat, the connection interface for attack route, assets protected from an attacker, location of threat, etc. can be imaged in a better way. Then, referring to the target range before, onboard devices connected or devices carried in the vehicle such as connection interface with external systems and onboard head units and are listed. A draft of the model for review was prepared.



* The charge system is not applicable and not shown on the figure.

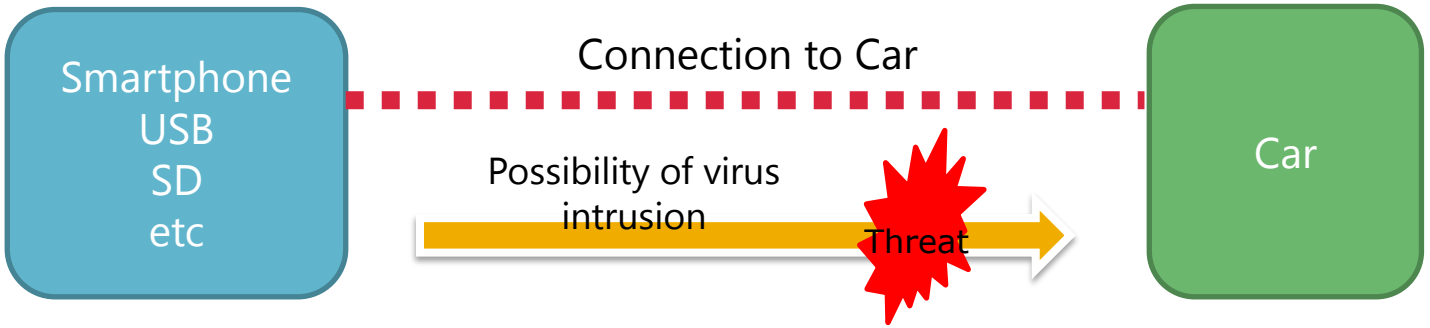
Onboard unit
Anticipated threat

■ Anticipated threat and damage

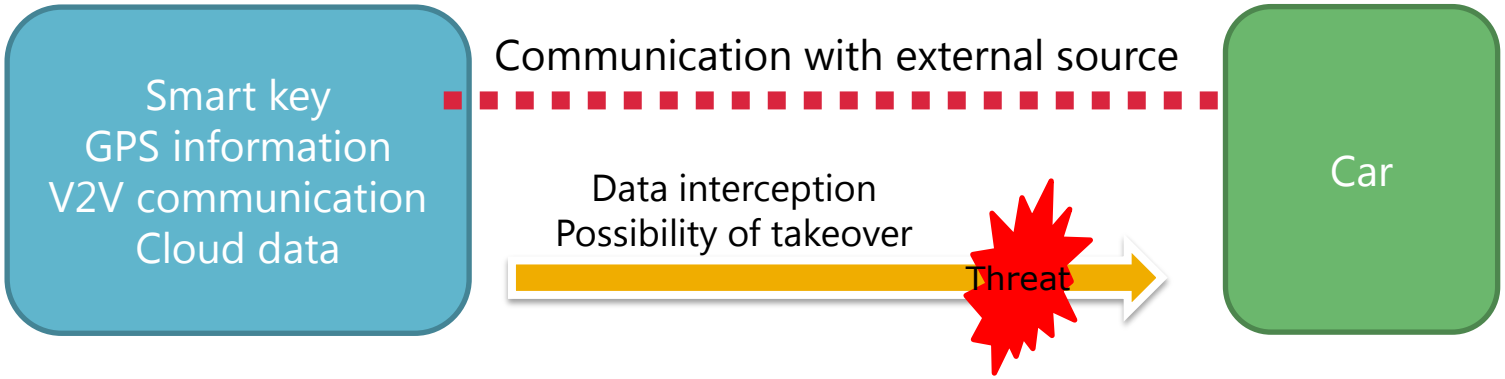
Item No.	Anticipated threat	Anticipated damage
1	DoS attack to onboard network through external network	Stop of all services requiring communication function
2	Transmission of false message by server spoofing	Confusion of users, etc.
3	Sniffing communication message using a third party receiver	Use for unintended service by the operation control institute
4	Distribution of message including incorrect position by abusing a third party GPS signal generator	Occurrence of confusion by message distribution including incorrect position
5	Spoofing of other onboard unit by abusing an onboard unit from a user, or by using a third party communication unit	Confusion by distribution of driving information including incorrect information
6	Spoofing of roadside unit by abusing an onboard unit from a user, or by using a third party communication unit (roadside unit spoofing)	Confusion by distribution of message including incorrect information
7	Tracing of person's position from the receiving message by using a third party receiver or by abusing an onboard unit from a user	Personal profiling
8	A third party intentionally stops the ECU control function in normal operation from the 3G/LTE line.	ECU operation is disabled and the vehicle function is disabled.
9	The vehicle status information is altered from a Bluetooth device such as smartphone by a dealer personnel during maintenance.	The settings are illegally changed and unintended change of the performance is made.
10	In normal operation, a third party intentionally causes malfunction of the information ECU function from the SD card interface.	Normal operation of the information function is disabled.

For in-vehicle
3.Assumed threat

- Equipment of BYOD (Bring your own device)



- External network



Threat analysis

■ Items of risk characteristics

Item No.	Item	Details
1	Target device	Device exposed to threat
2	Unique to field/common	Reference ☞ "(1) Unique to field/common"
3	Classification of threat	List examples of threat classifications. Reference ☞ "(2) Threat classification" The classification criteria are as follows: **(1) Attributable to operation of user** **⇒ "Setting error/virus infection"** **(2) Attack method by an attacker is obvious.** **⇒ "Sniffing/Dos attack/false message/illegal relay"** **(3) If the attack method by an attacker is not clear or the system suffers from damage not applicable to the above, the item below is applicable.** **⇒ "Illegal setting/information leak/lost log"** **If (1) or (2) above is not applicable, "illegal use" is determined.**
4	Connection I/F (intrusion route)	Reference ☞ "(3) Connection I/F (intrusion route)"
5	Who made the connection	Reference ☞ "(4) Who made the connection"
6	Whom suffers from damage	Reference ☞ "(5) Whom suffers from damage"
7	Where did it occur	Reference ☞ "(6) Where did it occur"

Trend analysis (classification of threat)

◇ Classification of threats

	Must	High	Middle	Low	Total count	Average risk value	M&H comparison
Setting error	2	0	2	0	4	14.8	50.0%
Virus infection	14	7	8	0	29	17.3	72.4%
Illegal use	33	18	10	2	63	18.0	81.0%
Illegal settings	3	8	2	2	15	14.4	73.3%
Information leak	0	1	1	6	8	7.2	12.5%
Sniffing	3	3	2	2	10	13.2	60.0%
Dos attack	21	12	18	3	54	15.1	61.1%
False message	17	16	4	0	37	19.5	89.2%
Lost log	0	0	0	1	1	7.5	0.0%
Illegal relay	1	5	5	0	11	12.5	54.5%

Total number of threats: 232

Illegal use: Threat which uses the function of the automobile system by an unauthorized person due to spoofing or attack on device vulnerability

False message: Threat which gives illegal operation or display on the automobile system by sending a spoofing message from an attacker.

* Classification of threat: Source Action guide (IPA) on automobile information security

Trend analysis (connection I/F)

Connection I/F (Intrusion route)

	Must	High	Middle	Low	TTL 件数合計	Ave of risk リスク値平均	M&H ratio M&H比率
3G/GSM	17	15	12	3	47	16.4	68.1%
Bluetooth	7	3	2	0	12	18.4	83.3%
CD	1	2	0	0	3	20.8	100.0%
DSRC	0	3	0	0	3	15.4	100.0%
E-call service interface	1	2	0	0	3	16.3	100.0%
GPS	4	4	1	0	9	17.4	88.9%
OBD	25	8	11	4	48	16.4	68.8%
RF	13	11	2	2	28	18.3	85.7%
SD	2	0	3	0	5	16.0	40.0%
USB	2	3	4	0	9	14.3	55.6%
VICS	0	3	0	0	3	15.4	100.0%
Wi-Fi	12	11	12	2	37	15.5	62.2%
Sensor	2	0	0	0	2	18.8	100.0%
Charging station	0	0	1	0	1	10.0	0.0%
Special equipment	6	5	4	5	20	12.9	55.0%

227
the total number of cases

Risk Assessment of Threats on “Connected Car”

Methods of Risk evaluation

In risk evaluation of threat examples, the risk evaluation methods related to onboard units were investigated from automobile related references.

1) Modified method of ETSI

The risk evaluation of ETSI (European Telecommunications Standard Institute) is classified into "Occurrence possibility" and "Effect". It is a method to classify the risk values with the product of values evaluated in 3 levels.

2) CRSS method (application of CVSS)

CRSS (CVSS based Risk Scoring System) is a risk evaluation method applying CVSS (Common Vulnerability Scoring System) which has been a proven risk evaluation method in vulnerability evaluation for information system/unit.

3) RSMA method

RSMA (Risk Scoring Methodology for Automotive system) is a method to determine the "risk value" into "effect" and "occurrence possibility" with the risk level sheet. The level of "Effect" is determined after classification into 3 damage types of "safety", "personal information/privacy" and "asset/company value".

4) CCDS improvement method

In CCDS, the method to rank the "risk value" for attack "difficulty" and "effect" for user is used. In the evaluation items, the basic axes are "difficulty" and "effect" to make early evaluation and development at the initial stage (refer to the general information of "Common Vulnerability Scoring System").

Risk characteristics used for evaluation

Item No.	Item	Details
1	Target device	Devices exposed to threat
2	Unique to field/common	Examples specific to vehicle field are classified to "unique to field". Examples which may occur in other IoT devices are classified to "common".
3	Classification of threat	Referring to classification examples in IPA "Action guide on automobile information security", 10 types of threats are classified.
4	Connection I/F (intrusion route)	Route intruded by threat
5	Who made the connection?	Referring to risk characteristics in IPA "Development guideline of connecting world", classify the person who made the connection.
6	Whom suffered from damage?	Referring to risk characteristics in IPA "Development guideline of connecting world", classify the target for damage.
7	Where did it occur?	Referring to risk characteristics in IPA "Development guideline of connecting world", classify the location of risk.

Risk evaluation example analyzed by onboard SWG

- About 230 threat examples are collected from Japanese/overseas documents for risk evaluation.

Examples of threats			Risk characteristics						
Examples	Anticipated threat	Anticipated damage	Target device	Unique to field/ common	Classification of threat	Connection I/F (intrusion route)	Who made the connection ?	Whom suffered from damage?	Where did it occur?
1	DoS attack on onboard network through external network	Stop of all services requiring communication function	Onboard unit	Common	DoS attack	3G/GSM	Attacker	IoT function	I/F normally used
2	Transmission false message by server spoofing	Confusion of user, etc.	Onboard unit	Common	False message	3G/GSM	User (error connection)	IoT function	I/F normally used
3	System freeze with streaming contents using browser bug	Stop of infotainment based services	Onboard unit	Common	False message	3G/GSM	User (intentional)	IoT function	I/F normally used
4	Sniffing of communication message using a receiver by a third party	Use for unintended service by operation control agency	Onboard unit	Common	Sniffing	Wi-Fi	Attacker	Information	I/F normally used
5	Distribution of message including incorrect position by abusing a third party GPS signal generator	Confusion by message distribution including incorrect position	Onboard unit	Common	Illegal relay	GPS	Attacker	Original function	I/F normally used
6	Spoofing of roadside unit by abusing an onboard unit from a user, or by using a third party communication unit	Confusion by distribution of driving information including incorrect information	Onboard unit	Common	Illegal use	3G/GSM	User (intentional)	Information	I/F normally used
7	Tracing of person's position from the receiving message by using a third party receiver or by abusing an onboard unit from a user	Personal profiling	Onboard unit	Specific to field	Information leak	Wi-Fi	Attacker	Information	I/F normally used
8	A third party intentionally stops the ECU control function in normal operation from the 3G/LTE line.	ECU operation is disabled and the vehicle function is disabled.	ECU	Specific to field	Illegal use	3G/GSM	Attacker	Original function	I/F normally used
9	The vehicle status information is altered from a Bluetooth device such as smartphone by a dealer personnel during maintenance.	The settings are illegally changed and unintended change of the performance is made.	Onboard unit	Specific to field	Illegal setting	Bluetooth	Service provider	Information	I/F normally used
10	In normal operation, a third party intentionally causes malfunction of the information ECU function from the SD card interface.	Normal operation of the information function is disabled.	ECU	Specific to field	Illegal use	SD	Attacker	Original function	I/F normally used

Risk evaluation example analyzed by onboard SWG

■ About 230 threat examples are collected from Japanese/overseas documents for risk evaluation.

Examples of threats			Risk characteristics							Comparison of risk values			
Examples	Anticipated threat	Anticipated damage	Target device	Unique to field/ common	Classification of threat	Connection I/F (intrusion route)	Who made the connection ?	Whom suffered from damage?	Where did it occur?	Improvement method of ETSI	CRSS (application of CVSS)	RSMA method	CCDS improvement method
1	DoS attack on onboard network through external network	Stop of all services requiring communication function	Onboard unit	Common	DoS attack	3G/GSM	Attacker	IoT function	I/F normally used	Critical (6)	Level II (warning)	H	Must
2	Transmission false message by server spoofing	Confusion of user, etc.	Onboard unit	Common	False message	3G/GSM	User (error connection)	IoT function	I/F normally used	Major (4)	Level II (warning)	M	High
3	System freeze with streaming contents using browser bug	Stop of infotainment based services	Onboard unit	Common	False message	3G/GSM	User (intentional)	IoT function	I/F normally used	Major (4)	Level II (warning)	M	High
4	Sniffing of communication message using a receiver by a third party	Use for unintended service by operation control agency	Onboard unit	Common	Sniffing	Wi-Fi	Attacker	Information	I/F normally used	Minor (3)	Level I (caution)	L	Low
5	Distribution of message including incorrect position by abusing a third party GPS signal generator	Confusion by message distribution including incorrect position	Onboard unit	Common	Illegal relay	GPS	Attacker	Original function	I/F normally used	Major (4)	Level II (warning)	H	Middle
6	Spoofing of roadside unit by abusing an onboard unit from a user, or by using a third party communication unit	Confusion by distribution of driving information including incorrect information	Onboard unit	Common	Illegal use	3G/GSM	User (intentional)	Information	I/F normally used	Major (4)	Level II (warning)	M	Middle
7	Tracing of person's position from the receiving message by using a third party receiver or by abusing an onboard unit from a user	Personal profiling	Onboard unit	Specific to field	Information leak	Wi-Fi	Attacker	Information	I/F normally used	Minor (3)	Level I (caution)	L	Low
8	A third party intentionally stops the ECU control function in normal operation from the 3G/LTE line.	ECU operation is disabled and the vehicle function is disabled.	ECU	Specific to field	Illegal use	3G/GSM	Attacker	Original function	I/F normally used	Critical (6)	Level III (danger)	H	Must
9	The vehicle status information is altered from a Bluetooth device such as smartphone by a dealer personnel during maintenance.	The settings are illegally changed and unintended change of the performance is made.	Onboard unit	Specific to field	Illegal setting	Bluetooth	Service provider	Information	I/F normally used	Major (4)	Level II (warning)	M	High
10	In normal operation, a third party intentionally causes malfunction of the information ECU function from the SD card interface.	Normal operation of the information function is disabled.	ECU	Specific to field	Illegal use	SD	Attacker	Original function	I/F normally used	Minor (3)	Level I (caution)	L	Middle

Validation Check of Risk Evaluation methods based on the recent vulnerable cases

最近発表の脅威事例 –その1–

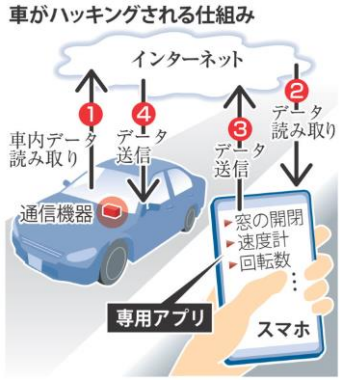
JEEP

■ 遠隔から車載LANに侵入した研
（昨年8月のBlack

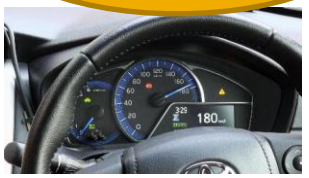
最近発表の脅威事例 –その2–

CAN message injection

■ スマホで車を遠隔操作する研究
（昨年12月のIoTセキュリティウィ



※毎日新聞の記事を参照



遠隔操作で窓を開閉させたり、停止中に速度表示を180キロにしたりできた

最近発表の脅威事例 –その3–

EV mobile apps

■ 電気自動車の専用アプリに脆弱性
他人の車を
（今年2月にオーストラリアの

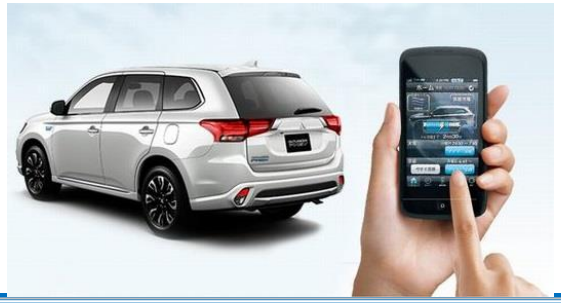
オーストラリアからインターネット経由で、英国にある電気自動車のエアコンやファンを作動させたり、運転履歴を取得することができた

最近発表の脅威事例 –その4–

PHEV mobile apps

■ PHEV車がスマホ等で外部から
セキュリティ企業が指摘

PHEV車をモバイルアプリで遠隔操作でき
を突いて車のライトやエアコンを付けたり盗難警報を解除したりできてしまうことが分かったとセキュリティ企業が伝えた。



◇メーカーHPの告知内容

第三者が無線LAN通信のパスワードを解読し、当該機能を不正にコントロールする事例が確認されました。（盗難防止アラームの解除、ヘッドランプやエアコンのＯＮ／ＯＦＦ操作、タイマー充電の設定変更）
現在のところ、ドア解錠やパワースイッチのコントロール、個人情報漏洩などの事例は確認されておりませんが、ご心配のお客様は全登録情報の削除の手順に従い、機能を停止下さい。
お客様にはご心配をおかけし、申し訳ございません。現在、無線LAN通信のセキュリティ性をより向上する対応を検討中です。

Risk evaluation example of threat recently released

- Threat examples 1 to 4 recently released are evaluated for risk.

Latest example of threat			Risk characteristics							Comparison of risk values			
Item No.	Anticipated threat	ated	Target device	Unique to field/ common	Classification of threat	Connection I/F (intrusion route)	Who made the connection ?	Whom suffered from damage?	Where did it occur?	Improvement method of ETSI	CRSS (application of CVSS)	RSMA method	CCDS improvement method
01	Intrusion in an onb unit is made through a mobile unit, the firmwar of the chip connected to CAN is rewritten and command is rem sent to CAN.	Steering wheel or engine is illegally	Onboard unit	Specific to field	Illegal use	3G/GSM	Attacker	Original function	I/F normally used	Critical (6)	Level III (danger)	H	Must
02	Device connecting to internet is connected to CAN and spoofing attack is made thro a smartphone.	opening/closing or speed display is ted.	ECU	Specific to field	Illegal use	3G/GSM	Attacker	Original function	Non-proper I/F	Critical (6)	Level III (danger)	H	Must
03	Vulnerability of the authentication system provided by a vehicle manufacturer is attacked and access to the vehi is gained through It is remotely ope	llegal operation of air-conditioner or fan, or	ECU	Specific to field	Illegal use	3G/GSM	Attacker	Original function	I/F normally used	Critical (6)	Level III (danger)	H	Must
04	Password of wireles communication is read by a third party. The function which can be remotely operated with mobile app of the PHEV vehicle is illegally controlled.	ehicle lights or air-conditioner or cancelling anti-theft alarm	ECU	Specific to field	Illegal use	Wi-Fi	Attacker	Original function	I/F normally used	Critical (6)	Level II (warning)	H	Must

JEEP

CAN message Injection

EV mobile apps

PHEV mobile apps

Risk evaluation example analyzed by onboard SWG

■ About 230 threat examples are collected from Japanese/overseas documents for risk evaluation.

Examples of threats			Risk characteristics							Comparison of risk values			
Examples	Anticipated threat	Anticipated damage	Target device	Unique to field/ common	Classification of threat	Connection I/F (intrusion route)	Who made the connection	Whom suffered from damage?	Where did it occur?	Improvement method of ETSI	CRSS (application of CVSS)	RSMA method	CCDS improvement method
1	DoS attack on onboard network through external network	Stop of all services requiring communication function	Onboard unit	Common	DoS attack	3G/GSM	Attacker	IoT function	I/F normally used	Critical (6)	Level II (warning)	H	Must
2	Transmission false message by server spoofing	Confusion of user, etc.	Onboard unit	Common	False message	3G/GSM	User (error connection)	IoT function	I/F normally used	Major (4)	Level II (warning)	M	High
3	System freeze with streaming contents using browser bug	Stop of infotainment based services	Onboard unit	Common	False message	3G/GSM	User (intentional)	IoT function	I/F normally used	Major (4)	Level II (warning)	M	High
4	Sniffing of communication message using a receiver by a third party	Use for unintended service by operation control agency	Onboard unit	Common	Sniffing	Wi-Fi	Attacker	Information	I/F normally used	Minor (3)	Level I (caution)	L	Low
5	Distribution of message including incorrect position by abusing a third party GPS signal generator	Confusion by message distribution including incorrect position	Onboard unit	Common	Illegal relay	GPS	Attacker	Original function	I/F normally used	Major (4)	Level II (warning)	H	Middle
6	Spoofing of roadside unit by abusing an onboard unit from a user, or by using a third party communication unit	Confusion by distribution of driving information including incorrect information	Onboard unit	Common	Illegal use	3G/GSM	User (intentional)	Information	I/F normally used	Major (4)	Level II (warning)	M	Middle
7	Tracing of person's position from the receiving message by using a third party receiver or by abusing an onboard unit from a user	Personal profiling	Onboard unit	Specific to field	Information leak	Wi-Fi	Attacker	Information	I/F normally used	Minor (3)	Level I (caution)	L	Low
8	A third party intentionally stops the ECU control function in normal operation from the 3G/LTE line.	ECU operation is disabled and the vehicle function is disabled.	ECU	Specific to field	Illegal use	3G/GSM	Attacker	Original function	I/F normally used	Critical (6)	Level III (danger)	H	Must
9	The vehicle status information is altered from a Bluetooth device such as smartphone by a dealer personnel during maintenance.	The settings are illegally changed and unintended change of the performance is made.	Onboard unit	Specific to field	Illegal setting	Bluetooth	Service provider	Information	I/F normally used	Major (4)	Level II (warning)	M	High
10	In normal operation, a third party intentionally causes malfunction of the information ECU function from the SD card interface.	Normal operation of the information function is disabled.	ECU	Specific to field	Illegal use	SD	Attacker	Original function	I/F normally used	Minor (3)	Level I (caution)	L	Middle

Value of Countermeasures

Value of Countermeasures should evaluated by the effect of Risk Reduction values.

■ Threat Analysis before applying countermeasures

区分	Must	High	Middle	Low	M&H 比率
Setting error	2	0	2	0	50.0%
Virus infection	14	7	8	0	72.4%
Illegal use	33	18	10	2	81.0%
Illegal settings	3	8	2	2	73.3%
Information leak	0	1	1	6	12.5%
Sniffing	3	3	2	2	60.0%
Dos attack	21	12	18	3	61.1%
False message	17	16	3	0	91.7%
Lost log	0	0	0	1	0.0%
Illegal relay	1	5	5	0	54.5%

Re-evaluation after countermeasures

Must	High	Middle	Low	M&H 比率
0	2	2	0	50.0%
12	7	10	0	65.5%
27	9	23	4	57.1%
0	6	6	0	50.0%
0	1	1	6	12.5%
0	4	2	4	40.0%
13	8	28	5	38.9%
13	4	17	2	47.2%
0	0	0	1	0.0%
1	5	5	0	54.5%

Summary

- CCDS Guideline WG, Car-SWG studied the threats analysis and risk assessment.

- There are some interesting results:
  - Some trends in threats
  - Four assessment methods likely the same

- Countermeasure value could be measured by comparing to the degrading value of risk before buying the countermeasure technology.

Thank you for your kind attention.