Study on Vulnerability Rating of the Intelligent and Connected Vehicle’s Cybersecurity

Yangyang Liu¹³, Zhao Wang², Yanan Zhang¹, Peiji Shi¹ and Xuebin Shao¹

¹ Automotive Data Center, China Automotive Technology and Research Center Co., Ltd., Tianjin, China.
² Auto Standardization Research Institute, China Automotive Technology and Research Center Co., Ltd., Tianjin, China.
³ Supported by program of scientific and technological activities for the returned Chinese who study abroad in Tianjin.

Abstract. Based on the automobile vulnerability data, the rating system of automobile cybersecurity vulnerabilities was constructed by referring to CIA, HEAVENS et al. First of all, basic rules such as naming, coding, classification and description of vulnerabilities are developed to ensure the uniqueness, normalization and compatibility of vulnerabilities. Next, the vulnerability rating system was developed by taking the three elements of scene, threat and impact and the 13 sub-elements of subdivision as evaluation indexes. The evaluation of the existing vulnerabilities and the comparison with the professional evaluation by using the established rating system show that the system is reasonable and effective.

1. Foreword
Since the beginning of the 21th century, automobiles have kept developing toward a direction of electrification, intellectualization, net connection and sharing, in which background intelligent connected vehicles emerge at the right moment. As a development direction of automobile industry, intelligent connected vehicle will again impact the pattern of the automobile industry and our trip mode, but also bring us corresponding threats on cybersecurity. Some hackers take use of automobile vulnerabilities to send out malicious codes to attack the intelligent connected vehicle, or even endanger personal safety and social security. To build a comprehensive and efficient intelligent automobile cybersecurity system, the promotion of automobile cybersecurity vulnerability level system is imperative [1]. There are vulnerability databases operating at home and broad already [2-3], but there is no relevant standard or specification grading of automobile vulnerabilities. Moreover, the grading of vulnerabilities is critical to vulnerability management, risk assessment and emergency response. Therefore, the study on automobile cybersecurity vulnerability level evaluation system is extremely urgent [4].

2. Significance of the establishment of automobile vulnerability level system
Along with the application of emerging technologies such as Internet, Artificial Intelligence, wireless network, cloud computing, big data and so on, degree of intellectualization and net connection of automobile has kept on growing. Automobile has become a veritable intelligent terminal device in the Internet Era and the cybersecurity of automobile will always be a problem requiring great attention in intelligent connected vehicles. Automobile cybersecurity now is still in a relatively preliminary state
which is easily to be broken through. Numerous works are still required, among which the threat analysis for cybersecurity is more complicate and important. For the whole vehicle and various sub-net components, there are too many unknown vulnerabilities and attacking modes. We need to put ourselves on attackers’ position to analyze with non-traditional vulnerability analysis, osmotic and statistical techniques, which is relatively difficult for traditional auto workers. Thus, a vulnerability grading system shall be developed to provide reference for whole vehicle cybersecurity evaluation, emergency response level constitution and so on, so as to take actions beforehand to prevent malicious use of vehicle vulnerabilities which may cause problems such as economic loss, driving mistake, stealing of privacy and damage on functional security.

From the view of automobile emergency response, when cybersecurity event occurs on intelligent connected vehicle, we need a set of feasible auto emergency response scheme to reduce response time as much as possible, so that we can respond quickly to mitigate or eliminate impact caused by the security event. According to the vulnerability level system, different repair modes are constituted for vulnerabilities in different levels, studies on emergency response mechanism are carried out and loss caused by improper vulnerability handling is reduced. Finally, whether the vulnerability is repaired is verified, and lessons learned are concluded and analyzed, which provide reference for vulnerability emergency response and security development in future.

From the view of auto vulnerability management, risk assessment can be carried out on vulnerabilities to evaluate the probability for intelligent connected vehicles to suffer threats and influence on road participants after their occurrence, as well as output a series of threats with corresponding risk levels. It can test the severity of vulnerabilities, rate and divide levels of security vulnerabilities preliminarily, as well as help applicators to determine the urgency and importance of response required by vulnerabilities.

3. Vulnerability level system

3.1. Basic rules of vulnerability level system

This part introduces basic rules of auto vulnerabilities including coding, naming, classification, description and so on.

3.1.1. Coding of auto vulnerabilities

To facilitate the identification and reflection of uniqueness, normativeness and compatibility of auto vulnerability data, unique codes are distributed to auto vulnerabilities indexed uniformly. The following principles shall be observed: 1) uniqueness: code for each auto vulnerability data shall be unique; 2) chronological order: it shall be easy to identify time of auto vulnerability indexing and define timeliness of vulnerabilities; 3) confidentiality: it shall be avoided to disclose business information in codes. According to the above principles, the following grammatical rule for coding is constituted: QCLD+YYYYMMDD+form code of any figure, i.e. “QCLD” is a fixed 4-bit code; “YYYY” is a four-bit sequenced code; “MM” is a two-bit sequenced code; “DD” is a two-bit sequenced code; “any figure” is a three-bit code ordered according to the sequence of generation of auto vulnerability, of which the quantity can be expanded when necessary, e.g.: QCLD-20180801-001, QCLD-20180801-1000.

3.1.2. Naming of auto vulnerabilities

Based on the coding of auto vulnerabilities, auto vulnerability data shall be named to facilitate retrieval and consultation [4]. Therefore, the following principles are constituted: 1) readability: it shall cover information related to the auto vulnerability data such as auto OEM, component manufacturer, auto service provider and auto model, sub-type of vulnerability and so on; 2) confidentiality: it shall be avoided to disclose any detail of the vulnerability technique. According to the above principles, the following naming method is proposed: “auto manufacturer” + “auto model name” + “vulnerability position”. Besides, “vulnerability” or “defect” is postfix at the end. Wherein,
name of manufacturer refers to short name of the manufacturer of the vehicle affected by the vulnerability. If the manufacturer usually uses Chinese name or if it is a foreign company without Chinese name, English name of the company will be adopted; vehicle name refers to the official name of the vehicle model affected by the vulnerability; vulnerability position refers to the specific position of the vehicle affected by the vulnerability. For example: XX company XX vehicle steering lamp defect.

3.1.3. Classification of auto vulnerabilities
The utilization of auto vulnerability is generally not possible by single component only. It requires the use of a series of combined defects on different components. Therefore, the classification of auto vulnerabilities based on defective object module may cause unclear classification [5-7]. According to concepts of threat and property in cybersecurity, two parameters are designed - vulnerability component and affected components.

Vulnerability component refers to vehicle components containing defects. It is a kind of threat. Attackers attack vehicle by using vulnerabilities in vulnerability components;

Affected component refers to components endangered after successful use of vehicle vulnerabilities. It is a kind of property. Affected component can be the vulnerability component itself, or other software, hardware or network components in the vehicle.

This auto cybersecurity vulnerability system is based on vulnerability components. It classifies auto vulnerabilities into seven categories (APP, cloud platform, IVI, T-BOX, radio, ECU, bus and so on) according to threat analysis on cybersecurity of intelligent connected vehicles.

![Vulnerability types](image1)

Figure 1 Vulnerability types

3.1.4. Description of auto vulnerabilities
For vulnerability data confirmed to be indexed, text description shall be adopted to describe cause, existing position, affected range and so on of the vulnerability in a uniform format. According to the above requirements, the following principles are constituted: 1) simplicity: describe the vulnerability simply, clearly and straightforward; 2) authenticity: describe the vulnerability truly and objectively; 3) confidentiality: avoid to disclose excessive technical details of the vulnerability which may cause secondary hazard. According to the above principles, method for content description is constituted:

The method for auto vulnerability data description includes “vulnerability body introduction” and “vulnerability content introduction”. In the “vulnerability body introduction”, it is required to sketch basic information of the system or product where the vulnerability exists, which includes “name of the vulnerability body”, “name of the vehicle related company”, “definition of the vulnerability body”, “functional overview”, e.g.: XXX is a XXX product (software, solution, system, tool and so on) of XXX (English) Company in XXX (country). The product possesses function of XXX; in the “vulnerability content introduction”, it is required to sketch type, cause, attacking mode and impact of
the vulnerability, including “type of vulnerability”, “cause”, “use manner”, “impact and consequence”. E.g.: this car has XX (type) type vulnerability which is caused by XX of XX (name of the product or system). Attackers can fulfill XX attack via XX (manner) to cause XX danger or result.

3.2. Vulnerability level evaluation system

With reference to cybersecurity CIA model, HEAVENS model, CVSS model and real vehicle tests, 3 categories of parameters and 13 types of sub-parameters are summarized and stated in a tree structure[8-10]. Among sub-factors, different to the static grading made by traditional Internet on vulnerabilities, dynamic factors are added (e.g. danger time) to reduce uncertainty brought to risk assessment, emergency response and so on.

![Figure 2 Tree structure for vulnerability rating parameters](image)

3.2.1. Scene parameters (SP)

The evaluation factor “scene parameter” refers to the correlation factors describing state and range of the affected vehicle by using relevant technical mastery situation when the vulnerability is attacking the vehicle. Three kinds of sub-factors are set: technical mastery, vehicle condition and scope of attack:

1) Technical mastery refers to the comprehensive consideration on the understanding on the attacking vulnerability used and mastery degree on technology;

2) Vehicle condition refers to the state of vehicle when attacked, distinguished by driving speed;

3) Scope of attack refers to the comprehensive consideration on quantities and varieties of auto targets attacked;

Levels, corresponding definitions and benchmark value of sub-factors are as following:

| Parameter name       | Level | Description                                                                 | Score |
|----------------------|-------|-----------------------------------------------------------------------------|-------|
| Technical mastery (TM) | Low   | Dimly aware position of vulnerability; master attack flow including attacking tools, attack steps and so on | 1     |
|                      | Medium| Can acquire vulnerability material and information in details; know relevant principles of the vulnerability in a “low” level | 3     |
|                      | High  | Be proficient on the work mode of vulnerability triggering in a “medium” level; mature principles have been accumulated | 10    |
| Vehicle              | Still | The car is parking or idling, i.e. the car speed is 1 | 1     |
### Conditions (VC)

| Level              | Description                                      | Score |
|--------------------|--------------------------------------------------|-------|
| Low speed          | The car is driving in a speed of 0-15km/h        | 2     |
| Medium speed       | The car is driving in a speed of 16km/h to 25km/h | 4     |
| Relatively high speed | The car is driving in a speed of 26km/h to 50km/h | 7     |
| High speed         | The car is driving in a speed above 50km/h       | 10    |

### Attack area (AA)

| Attack type                  | Description                                                                 |
|------------------------------|-----------------------------------------------------------------------------|
| Single vehicle attack        | Launch vulnerability attack on one vehicle only                             | 1     |
| Single model attack          | Can use the vulnerability to attack same vehicle model                      | 7     |
| Multi model attack           | Can use the vulnerability to attack more than one vehicle models             | 10    |

Take the mined vulnerability data as study sample and use neural network modification formula coefficient to obtain the formula for calculation score for scene parameter:

\[
SP = 0.952 \times TM + 1.905 \times VC + 1.429 \times AA
\]  

Wherein: SP refers to the score of scene parameter; TM refers to the value taken for technical mastery parameter; VC refers to the value taken for vehicle condition parameter; AA refers to the value taken for the attacking area parameter.

#### 3.2.2. Threat parameter

The evaluation factor “threat parameter” refers to the correlation factors successfully triggering the vulnerability when an attack is launched for the vulnerability to be evaluated. It can be divided into four kinds of factors: window, knowledge and skill, equipment, scope of attack and so on:

1. Window refers to the attack vector adopted when using the vulnerability for attack;
2. Knowledge and skill refer to comprehensive consideration using basic principle, method, audience of knowledge groups and so on when an attack is launched;
3. Equipment refers to the advanced level of equipment used when mining and using vulnerabilities, as well as launching attacks;
4. Scope of attack refers to the quantity of component targets attacked by using the vulnerability when an attack is launched;

| Parameter name | Level               | Description                                                                 | Score |
|----------------|---------------------|-----------------------------------------------------------------------------|-------|
| Window (WD)    | Remote              | The attacker can launch attacks to automobile by using the vulnerability via the Internet, e.g. 4G, 3G and so on | 10    |
|                | Close range         | The attacker can use the vulnerability to attack automobiles by shared physical or logics, e.g.: bluetooth, Wi-Fi, IEEE 802.11, local IP subnet and so on | 5     |
|       | Local                                                                 | Physical contact                                                                 | Knowledge and skill (KS)                                                                 | Equipment (EM)                                                                 |
|-------|----------------------------------------------------------------------|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
|       | The attacker can use the vulnerability by reading/writing operations or running applications/tools, i.e. local participation is required for the use of vulnerability, for example: the attacker shall login locally; users shall download, accept the malicious contents | The attacker shall contact the automobile physically to launch an attack, for example, launch the attack on automobile bus by OBD II | Amateur | The attacker takes use of existing attack to execute simple command to launch attack but will not improve the attack method and attack tool |
|       |                                                                      |                                                                                  | Skillful operator                                                                     | Open hardware equipment and software |
|       |                                                                      |                                                                                  |                                                                      | The equipment used to launch attack has been publicly available, relatively common in traditional safety field, such as protocol analyzer, downloader, common IT equipment - notebook computer and so on |
|       |                                                                      |                                                                                  |Automobile safety expert                                                               | Open hardware equipment and software for specific use |
|       |                                                                      |                                                                                  |                                                                      | The equipment is not easy to be obtained by attackers; but its script can be attacked by purchasing or development; for example: on-board communication equipment, vehicle spy, CANoe, USRP and so on |
|       |                                                                      |                                                                                  | Multi-field expert                                                                     | Customize d or specific hardware equipment and software |
|       |                                                                      |                                                                                  |                                                                      | The equipment is specifically produced or especially complicate software; the equipment or software is under control, or very expensive, for example Unpacker ExeCryptor exclusively used by some national organizations |
|       |                                                                      |                                                                                  |                                                                      | Multiple customized or specific hardware equipment and software |
|       |                                                                      |                                                                                  |                                                                      | Equipment or software needs to be customized by different disciplines for different attack steps when the attacker launches attacks |
| Scope of | Single                                                               | Launch attack on unique component in the attacked vehicle |


Multiple Launch attack on more than one components in the attacked vehicle but not all components

Almost all Against all electronically-controlled components in the vehicle

Take the mined vulnerability data as study sample and use neural network modification formula coefficient to obtain the formula for calculation score for threat parameter:

\[ TP = 1.905 \times WD + 0.952 \times KS + 0.952 \times EM + 1.905 \times SA \]  

Wherein: TP refers to the score of threat parameter; WD refers to the value taken for window parameter; KS refers to the value taken for knowledge and skill parameter; EM refers to the value taken for equipment parameter; SA refers to the value taken for the scope of attack parameter.

### 3.2.3. Impact parameter

The evaluation factor “impact parameter” refers to the correlation factors related to dangers caused by attack on vehicles. They can be divided into six categories: personal safety, property, operation, privacy, public security and regulations, danger time and so on:

1. Personal safety refers to the severity of safety injury on people in the automobile;
2. Property refers to the total property consideration on direct and indirect losses caused to the automobile manufacturer, component manufacturer and individuals;
3. Operation refers to unexpected losses on automobile function after attack;
4. Privacy refers to losses caused by infringement on personal privacy after attack;
5. Public security and regulations refer to comprehensive consideration on losses caused by harm on surrounding public security and damage on laws and regulations;
6. Danger time refers to the duration of suffering by the vehicle after attack.

#### Table 3 Impact parameters

| Parameter name | Level  | Description                                                                 | Score |
|----------------|-------|-----------------------------------------------------------------------------|-------|
| Personal safety (PS) | NA    | No personal injury                                                          | 0     |
|                  | Minor injury | The driver and passengers are slightly injured but able to move freely | 3     |
|                  | Serious injury | The driver and passengers are not able to move freely                  | 7     |
|                  | Life threat   | Life crisis on the driver and passengers; or many people are injured        | 10    |
| Property (PP)    | NA    | No property loss                                                            | 0     |
|                  | Low   | Property loss on single vehicle                                             | 2     |
|                  | Medium | Property loss on multiple vehicles                                          | 6     |
|                  | High  | Huge property loss to the OEM or component manufacturer or even huge property loss to the national auto industry | 10    |
| Operation (OA)   | NA    | No operational impact                                                       | 0     |
|                  | Low   | Impact operation of entertainment system only                              | 2     |
|                  | Medium | Impact operation of body system                                             | 4     |
|                  | High  | Impact operation of power control system                                     | 10    |
| Privacy          | NA    | No loss of privacy data                                                     | 0     |
8

| (PA)         | Low                                              | Medium                                         | High                                             |
|--------------|--------------------------------------------------|------------------------------------------------|--------------------------------------------------|
| Public security and regulations (PR) | Infringe privacy data such as account, password, address book and so on of a single person | Infringe privacy data such as account, password, address book and so on of multiple persons | User privacy data of the whole vehicle model, whole OEM or even all vehicle manufacturers |
| NA           | No loss on public security and regulations       | Low                                            | Will not cause social harm; cause slight damage to laws and regulations |
| Low          | Will not cause social harm; cause slight damage to laws and regulations | Medium                                         | Cause slight social harm                         |
| Medium       | Cause slight social harm                         | High                                           | Cause serious social harm; cause serious damage to laws and regulations |
| High         | Cause serious social harm; cause serious damage to laws and regulations | NA                                             | Able to retrieve immediately after attack        |
| Short time   | Able to retrieve within several hours after attack | Low                                            | Able to retrieve one day or above after attack   |
| Long time    | Able to retrieve one day or above after attack   | Medium                                         | Not able to retrieve without interference from professionals after attack |
| Not able to retrieve | Not able to retrieve without interference from professionals after attack | High                                           | NA                                              |
| Danger time (DT) | NA                                             | Short time                                     | Long time                                       |
|              | Able to retrieve immediately after attack        | Able to retrieve within several hours after attack | Able to retrieve one day or above after attack   |
|              | Not able to retrieve without interference from professionals after attack | NA                                             | Long time                                       |

Take the mined vulnerability data as study sample and use neural network modification formula coefficient to obtain the formula for calculation score for impact parameter:

\[ IP = 3.333 \times PS + 1.429 \times PP + 0.952 \times OA + 0.953 \times PA + 2.381 \times PR + 0.952 \times DT \]  

(3)

Wherein: IP refers to the score of impact parameters; PS refers to value taken for personal safety parameter; PP refers to value taken for property parameter; OA refers to value taken for operation parameter; PA refers to value taken for privacy parameter; PR refers to value taken for public security and regulations parameter; DT refers to value taken for danger time parameter.

3.3. Vulnerability level

3.3.1. Attack level (AL)

Attack level is determined by the superposition of positive effects of scene parameters and threat parameters.

\[ AL = SP + TP \]  

(4)

Wherein: AL refers to the value taken for attack level parameter.

| Total of attack level parameter (AL) | Attack level | Score for attack level |
|-------------------------------------|--------------|------------------------|
| 0-15                                | Low          | 1                      |
| 16-40                               | Medium       | 2                      |
| 41-70                               | High         | 3                      |
| Above 70                            | Extremely high| 4                      |

3.3.2. Impact level (IL)

Impact level is determined by the function of impact parameters.
Wherein: IL refers to the value taken for impact level parameter.

### Table 5 Impact level evaluation form

| Total of impact level parameter (IL) | Impact level | Score of impact level |
|-------------------------------------|--------------|-----------------------|
| 0-15                                | Low          | 1                     |
| 16-40                               | Medium       | 2                     |
| 41-70                               | High         | 3                     |
| Above 70                            | Extremely high | 4                   |

3.3.3. Vulnerability level (VL)

Vulnerability level is determined according to the 2D diagram formed by impact level and attack level.

### Table 6 Vulnerability level rating form

| Vulnerability level (VL) | Impact level (IL) |
|--------------------------|-------------------|
| Attack level (AL)        | 1     | 2     | 3     | 4     |
| 1                        | Low risk | Low risk | Low risk | Medium risk |
| 2                        | Low risk | Medium risk | Medium risk | High risk |
| 3                        | Low risk | Medium risk | High risk | High risk |
| 4                        | Medium risk | High risk | High risk | Serious |

Wherein: VL refers to vulnerability level, including four levels: low risk, medium risk, high risk and serious.

4. Application of vulnerability level system

Famous hackers Charlie Miller and Chris Valasek in America fulfilled remote attack without physical contact on 2014 Jeep Cherokee produced by Chrysler. When the attack was launched, the hackers took use of a series of combined defects, including relevant vulnerabilities of OMAP-DM3730 system, V850 controller embedded in the on-board information interaction system, cellular network service defect of operator Sprint, open port D-Bus (6667) and so on. Finally, the hackers fulfilled the control over comfort system (such as air conditioning system), information and entertainment system (such as radio, IVI) and power control system (such as acceleration, steering) of the vehicle [11,12]. For the “Chrysler Jeep Cherokee auto power braking system remote controlled vulnerability”, the intelligent connected vehicle cybersecurity vulnerability level system was applied:

4.1. Scene parameter analysis

For “technical mastery” parameter: in relevant information available, it was only dimly known that the position of vulnerability of that vehicle was on the OMAP-DM3730 system and V850 controller embedded in the on-board information interaction system without knowing technical details on firmware level, therefore basis system was defined as “low”; for “vehicle condition” parameter: sudden braking and driving in a speed above 50km/h were realizable under a speed of 30km/h, as well as sudden loss of power for the vehicle and failure of accelerator. To sum up, it could be defined as “relatively high speed”; for “attack area” parameter, the vulnerability was not only accessible on 2014 Jeep Cherokee, but also on 2014 dodge Durango, thus was defined as “multi-model attack”.

According to formula (1), score of impact parameter is calculated as:

$$SP = 0.952 * 1 + 1.905 * 7 + 1.429 * 10 = 28.577$$  (6)
4.2. Threat parameter analysis
For “window” parameter: hackers took use of the vulnerability via Sprint cellular network, thus it was defined as “remote”; for “knowledge and skill” parameter: mining and use of this vulnerability required knowledge on multiple professional fields including software engineering, communication, cryptology, hardware and so on, thus it was defined as “multi-field expert”; for “equipment” parameter: when the hackers launched an attack, they used ordinary notebook computer; but in firmware study, firmware extraction and professional programmer required were required, thus it was defined as “open hardware equipment and software for specific use”; for “scope of attack” factor: the vulnerability not only enabled attack on electrically-controlled components related to power control system, but also brought impact to all electrically-controlled components on Jeep Cherokee cars, thus it was defined “almost all”. 

According to formula (2), score of threat parameter is calculated as:
\[
TP = 1.905 \times 10 + 0.952 \times 1 + 0.952 \times 3 + 1.905 \times 10 = 41.908
\] (7)

According to formula (4), score of attack level is calculated as:
\[
AL = SP + TP = 70.485
\] (8)

4.3. Impact parameter analysis
For “personal safety” parameter: when the power braking system was attacked, sudden braking might seriously threaten lives of the driver and passengers, thus it was defined as “life threat”; for “property” parameter: if the vulnerability was not repaired timely, Chrysler might suffer huge property loss, thus it was defined as “high”; for “operation” parameter: after the attack was launched, operation of power control system was affected, thus it was defined as “high”; for “privacy” parameter: the vulnerability didn’t involve privacy issues, thus it was defined as “NA”; for “public security and regulation” parameter: the vulnerability was applicable to multiple vehicle models and attack might cause sudden brake of multiple vehicles, causing serious social danger, thus it was defined as “high”; for “danger time” parameter: when the attack was launched, only malicious code was input into the on-board terminal. Once stop transmitting, the vehicle would retrieve. Thus it was defined “NA”.

According to formula (3), score of impact parameter is calculated as:
\[
IP = 3.333 \times 10 + 1.429 \times 10 + 0.952 \times 10 + 0.953 \times 0 + 2.381 \times 10 + 0.952 \times 0 = 80.95
\] (9)

According to formula (5), score of impact level is calculated as:
\[
IL = IP = 80.95
\] (10)

4.4. Vulnerability level evaluation
Score of attack level was 70.485, above 70, thus was defined “extremely high”; score of impact level was 80.950, above 70, thus was defined “extremely high”; according to the vulnerability level-rating form, the vulnerability was graded as “serious” level.

4.5. Application of vulnerability description
According to instance analysis, the weak component in this vulnerability was IVI system. According to the classification rule, the vulnerability was IVI type; according to coding rule, the vulnerability was coded as QCLD-20180728-001; according to the naming rule, the vulnerability was named “Vulnerability that Chrysler Jeep Cherokee auto power braking system was controlled remotely”; in the vulnerability description, for description on impacted components, key components involved in this vulnerability mainly included OMAP-DM3730 and V850 controller. OMAP-DM3730 is a processor based on open multi-media application platform OMAP produced by Texas Instruments (TI) in America. It is composed by 1GHz ARM Cortex-A8 Core and 800MHz TMS320C64x+DSP Core, and possesses functions such as 3D graphic processing and video acceleration; V850 is a micro-controller supporting real time operating system produced by Renesas (NEC) in Japan. For the description on vulnerability contents, the vehicle contained IVI type vulnerability which was caused by that the firmware updating of V850 micro-controller was not protected by signature mechanism and
attackers could adopt methods such as flash of V850 firmware, insertion of malicious code, and so on. Moreover, V850 under the high level could awake the OMAP, which fulfilled the conditions of remote control on acceleration, braking, and steering system of the vehicle, and could cause serious personal injury and property loss. The collection is as shown in the following figure:

Figure 3 Vulnerability Collection

5. Verification of Vulnerability Rating System

Comparison between grading of partial auto vulnerabilities by expert evaluation and the results from the vulnerability grading system is shown below:

Table 7 Vulnerability system verification

| NO. | Name of vulnerability                                      | Expert evaluation | System evaluation |
|-----|------------------------------------------------------------|-------------------|-------------------|
| 1   | XX1 In-car network Car flameout vulnerability caused by OBD | Low risk          | Low risk          |
| 2   | XX2 In-car network causes car flameout vulnerability by OBD | Low risk          | Low risk          |
| 3   | XX2 Vulnerability of diagnosis network controlling I/O identifiers | Low risk          | Low risk          |
| 4   | XX2 Wireless key signal hijacking vulnerability            | Medium risk       | High risk         |
| 5   | XX2 IVI contains external opening port vulnerability       | Medium risk       | Medium risk       |
| 6   | XX2 Cell phone APP installation package non-encrypted data vulnerability | Medium risk | Medium risk |
| 7   | XX2 Auto cloud platform contains sensitive information vulnerability | High risk | Medium risk |
| 8   | XX3 Cell phone APP account key data non-encryption vulnerability | Medium risk | Medium risk |
| 9   | XX5 In-car network triggers backup camera vulnerability by OBD | Medium risk | Medium risk |
| 10  | XX5 Vulnerability of diagnosis network reading               | Low risk          | Low risk          |
Among the 18 vulnerabilities verified, only the “XX2 auto wireless key signal hijacking vulnerability”, “XX2 auto cloud platform contains sensitive information vulnerability”, and “XX6 auto cloud platform contains injection vulnerability” are different. Results by expert evaluation are medium risk, high risk, high risk; while the results from the vulnerability system are high risk, medium risk, medium risk. Some parameter setting requires improvement, for example: vehicle condition. To sum up, the intelligent connected vehicle cybersecurity evaluation system can rationally and scientifically evaluate auto vulnerabilities.

6. Conclusions
This paper builds a set of intelligent connected vehicle cybersecurity vulnerability level system: 1. Fundamental rules: this part contains rules such as coding, naming, classification, description and so on. It can facilitate management of auto vulnerabilities; 2. Auto vulnerability level evaluation system: this part is based on models such as CIA, HEVENS and CVSS system. It constitutes an auto vulnerability level evaluation method containing three categories of factors (scene, threat and impact), totally 13 types of sub-factors. This system has broken the situation of no specification and standard for reference in grading of intelligent connected vehicle cybersecurity vulnerabilities. It provides a practical method for evaluation of auto vulnerabilities and certain theoretical supporting for construction of vulnerability database for use in autos, as well as guarantees cybersecurity of intelligent connected vehicles in certain degree.

References
[1] LIU Qi-xu, ZHANG Chong-bin, ZHANG Yu-qing, et al. Research on key technology of vulnerability threat classification[A]. Journal on Communications, 2012, 33(Z1): 79-87.
[2] National vulnerability Database. http:nvd.nist.gov/.
[3] Common Vulnerability Scoring System Version 3.0 Calculator. https://www.first.org/cvss/calculator/3.0.
[4] Common Vulnerabilities and Exposures (CVE). https://cve.mitre.org.
[5] The Open Source vulnerability Database. http:osvdb.org/.
[6] US-CERT vulnerability Notes Field Descriptions. http:www.kb.cert.org/vuls/html/fieldhelp/#help.
[7] SANS Critical vulnerability Analysis. http:www.sans.org/newsletters/cva/.
[8] WANG L, JAJODIA S, SINGHAL A, et al. K-zero-day safety: measuring the security risk of networks against unknown attacks[A]. 15th European Symposium on Research in Computer Security[C]. Athens, Greece, 2010. 573-587.

[9] T. Becsi, S. Aradi and P. Gaspar, “Security issues and vulnerabilities in connected car systems”, in Proc. 2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS 2015), pp. 477-482, 2015.

[10] FRUHWIRTH C, MANNISTO T. Improving CVSS-based vulnerability prioritization and response with context information[A]. 2009 3rd International Symposium on Empirical Software Engineering and Measurement[C]. Lake Buena Vista, FL, USA, 2009. 535-544.

[11] SAE International J3061. “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,” 2016.

[12] A. Bouard, M. Graf and B. Burgkhardt, “Middleware-based security and privacy for in-car integration of third-party applications”, 401:17-32, 2013.