A Study of The Risk Quantification Method of Cyber-Physical Systems focusing on Direct-Access Attacks to In-Vehicle Networks

Yasuyuki Kawanishi*, Hideaki Nishihara†, Hideki Yamamoto*, Nonmembers, Hirotaka Yoshida†, and Hiroyuki Inoue†, Members

SUMMARY: Cyber-physical systems, in which ICT systems and field devices are interconnected and interlocked, have become widespread. More threats need to be taken into consideration when designing the security of cyber-physical systems. Attackers may cause damage to the physical world by attacks which exploit vulnerabilities of ICT systems, while other attackers may use the weaknesses of physical boundaries to exploit ICT systems. Therefore, it is necessary to assess such risks of attacks properly.

A direct-access attack in the field of automobiles is the latter type of attacks where an attacker connects unauthorized equipment to an in-vehicle network directly and attempts unauthorized access. But it has been considered as less realistic and evaluated less risky than other threats via network entry points by conventional risk assessment methods. We focused on reassessing threats via direct access attacks in proposing effective security design procedures for cyber-physical systems based on a guideline for automobiles, JASO TP15002. In this paper, we focus on “fitting to a specific area or viewpoint” of such a cyber-physical system, and devise a new risk quantification method, RSS-CWSS_CPS based on CWSS, which is also a vulnerability evaluation standard for ICT systems. It can quantify the characteristics of the physical boundaries in cyber-physical systems.

key words: In-vehicle security, security design, risk analysis, TP15002, CWSS

1. Introduction

With the rise of new systems in recent years, new security risks need to be assessed. As a result of the recent popularization of information and communication technology (ICT) in control systems such as automobiles and factories, cyber-physical systems that integrate ICT systems and field devices which control actuators and sensors in the physical world have become widespread rapidly. Cyber-physical systems have two new security risks due to the fusion of ICT and physical aspects. One risk is the damage to the physical world by the attacks which exploit vulnerabilities of the ICT systems, and the other is the exploitation of the ICT systems through the weaknesses of the physical boundary. Therefore, it is necessary to consider such risks properly in security process.

To deal with these new risks, legislation and the standardization of such systems has become urgent in industry. At the United Nations world forum for harmonization of vehicle regulations Working Party 29 (WP.29) [1], writing of such legislation is underway. In the standardization, guidelines such as ISO/SAE 21434 [2] for automobiles and IEC 62443 [3][4] for industrial control systems are progressing concurrently. Cybersecurity Assurance Level (CAL) defined in ISO/SAE 21434 and Security Level (SL) in IEC 62443 are similar concept.

Püllen et al. also mentioned a trial to apply IEC 62443 to automotive systems in 2020 [5].

Especially in the automotive field, automotive systems are considered as advanced cyber-physical systems that are more closely linked to ICT. The 11 major manufacturing companies involved in the automobile field released a framework for the development, testing and validation of safe automated vehicles [6] in 2019, and ENISA also released a report which defined good practice for security of smart cars [7] in the same year. In 2020, the US Department of Transportation also published “Automated Vehicles 4.0” [8] as a new guideline for automated cars.

The process of creating requirement specifications for security at the design stage is called “security design.” This process is necessary to guarantee security before the product is released. There are also movements related to security design. The Common Criteria (CC) [9]-based cyber security certification scheme (EUCC) [10] has been promoted mainly in the EU, and a draft was released in 2021. In 2019, Maliatsos et al. also proposed selecting security requirements for connected vehicles on CC [11].

A direct-access attack to in-vehicle network is one of cases that should be considered in the security design of cyber-physical systems. It is an attack where the attacker connects unauthorized equipment to in-vehicle networks directly and attempts unauthorized access, and it is one of threats in which attackers use the weaknesses of the physical boundary to exploit ICT systems. This type of attacks had been regarded unrealistic at first, but in recent years, it has become recognized as an actual risk in car theft. In Japan, there was an incident in 2021, “CAN Invader” [12].

Kawanishi et al. focused on the JASO TP15002 guideline [13] for an interpretation of Common Criteria based security design procedures and used the method of using vulnerability evaluation criteria to quantify risk. They added some perspectives to the guideline and applied them to automotive systems and industrial control systems (ICSs) [14][15][16][17]. In that same period, ISO/SAE 21434 is already being standardized for security management, where...
the requirements (RQs) for threat analysis and risk assessment (TARA) are defined in the chapters 15. However, although TP15002 is a slightly old guideline, it has rational and useful procedures suitable for security design. In particular, its procedures are still useful for putting security assessment like the use case in ISO/SAE 21434 Annex H into concrete procedures.

Kawanishi et al. also proposed a 2-step risk evaluation, in which security threats are described and quantified by only three attack victims’ perspectives (called the “asset container method”) [15]. By the evaluation, critical threats are easily extracted by their risk scores and analyzed in detail. Specifically, by allocating multiple metrics of vulnerability evaluation criteria from the perspective of the victim of cyber-attacks, the physical structure of the cyber-physical system is interpreted.

The risk quantification method using vulnerability criteria has also been studied in some related works. The method of using CVSS (Common vulnerability scoring system) for risk analysis is a relatively popular. Kawanishi et al. started their research by using CRSS (CVSS based Risk Scoring System) in Appendix D of TP15002 as a risk quantification method [13][14]. Ko et al. used CVSS v2 (version 2) [18] for risk analysis of a smart grid system [19]. Ando et al. considered using CVSS v3 (version 3) [20] for their threat analysis of automotive systems [21]. H.Zhang et al. introduced an expanded system based on CVSS v2 for their threat analysis of automotive systems [22]. Y.Zhang et al. also used CEM [23] for a risk evaluation of an automotive system [24].

However, there were some inconveniences in these methods. For example, the number of metrics was too few or too many to interpret the characteristics of cyber-physical systems, and there were some uncertain metrics related to circumstances of attackers such as their abilities, their motives and environments. We had to find a new risk quantification method to interpret threats of cyber-physical systems only from attack victims’ perspectives.

In this paper, we focus on the issue “fitting to a specific area or viewpoint” mentioned as Issue 4 in Subsection 3.1 for appropriate assessment of security risks in security design. We introduce another risk scoring system (RSS) by customizing CWSS (Common weakness scoring system) [25], RSS-CWSS_CPS, to fill gaps in actual and evaluation results. RSS-CWSS_CPS uses more metrics than CRSS and can more clearly interpret characteristics about physical boundaries in cyber-physical systems. Then, we examine a case study of a direct access attack to an automobile and compare the results between RSS-CWSS_CPS and CRSS in the usefulness regarding Issue 4 “fitting to a specific area or viewpoint.” Finally, we further analyze how each method interprets the cyber-physical system and quantifies its risks.

This paper is organized as follows. In Section 2, we introduce preliminary work related to this paper. In Section 3, we identify our goal and approach focusing on direct-access attacks to in-vehicle networks. In Section 4, we conduct a case study on automotive systems, compare results RSS_CWSS_CPS and CRSS and consider how the analysis results change by using our method. In Section 5, we describe issues for future study. Finally, in Section 6, we present our conclusion.

2. Preliminary

2.1 Security Design Procedures based on JASO TP 15002

JASO TP15002 is a guideline for Common Criteria based security design procedures, released by the Society of Automotive Engineers of Japan (JSAE). TP15002 has the following five phases:

- **Phase 1: Definition of Target of Evaluation (TOE):** Structure, function and data are described both logically and physically.
- **Phase 2: Identification of the threats:** All threats are identified without overlooking anything.
- **Phase 3: Risk Analysis:** Security risks belonging to threats are properly quantified and analyzed in detail. Vulnerability evaluation criteria are recommended for risk quantification.
- **Phase 4: Security objective specification:** Security countermeasures are considered.
- **Phase 5: Security requirement specification:** Security requirements in CC are tied to their respective countermeasures.

2.2 Ideas for Efficient Risk Evaluation Methods

In phases 2 and 3 of the TP15002 procedure, Kawanishi et al. promoted an efficient risk evaluation method in [15][17]. They presented the following three ideas:

- **2-step risk evaluation:** Procedures in phases 2 and 3 are divided into 2 processes respectively to minimize the amount of work done by security specialists and reduce the total cost. The former is the screening process to identify critical threats, and the latter is the detailed analysis process by specialists.
- **Asset container method:** Method to identify threats using only three attack victims’ perspectives and to cover all possible attacks. Three perspectives are used: "where" and "at" that describe the attack path, and "asset" that describes the asset to be protected.
- **Customized risk quantification method:** Existing vulnerability evaluation criteria are customized to evaluate and quantify the structure and environment of TOE more appropriately.

Especially, “asset container method” has an important role. It is a method to define threats without ambiguity, in which “where” means entry point of TOE, “at” means internal module of TOE, and “asset” means function or information used in each module. These three perspectives consist of only from information that the attack victim can
Vulnerability evaluation criteria are originally used for the following equation with the six metrics defined in automotive systems. CVSS v2, and often used as a measure for measuring the severity of a software threat, but they were also used as criteria to evaluate cyber-physical systems. CRSS was shown as one of the methods for evaluating risks of vehicles in TP15002. CRSS is a method using base metrics of CVSS v2, and often used as a measure for automotive systems. CRSS calculates the score for a threat by the following equation with the six metrics defined in Table 1:

\[
R_r = f(EF) \cdot (0.6 \cdot EF + 0.4 \cdot AE - 1.5) \\
\text{where} \quad EF = 10 \cdot (1 - (1-C) \cdot (1-I) \cdot (1-A)), \\
AE = 20 \cdot AV \cdot AC \cdot Au, \\
f(x) = 0 \text{ if } x = 0, 1.176 \text{ if } x \neq 0.
\]

In this paper, we choose CRSS as the conventional method to compare. CRSS is a popular method to evaluate automotive systems, and it is suitable for comparing differences with RSS-CWSS_CPS because it can allocate metrics appropriately when using the asset container method.

Although we also tried to choose a method based on CVSS v3, the later version, to compare as a conventional method, but rejected for two reasons:

- CVSS v3 is not suitable for the asset container method because some metrics need to imagine attackers’ perspectives such as PR (Privileges Required), UI (User Interaction) and S (Scope). Consideration of these metrics is out of scope, and it is difficult to compare differences.
- The number of AC ranks in CVSS v3 has been reduced from 3 to 2. In comparing the evaluation of attack complexity of direct-access attacks, CVSS v3 will be lower than CVSS v2.

### 3. Our Goal and Approach of this paper

#### 3.1 Issues and Our Goal in This Paper

Our research is to establish an effective security design method based on TP15002, and we have the following issues:

1. **Guarantee of threat coverage**: It is necessary to guarantee that all threats can be considered.
2. **Management of work not depending on expertise**: There is not enough budget or time to do all security design work with only experienced security experts.
3. **Time, cost, and resource optimization**: It is desirable to save time and money by minimizing the processes that require specialists.
4. **Fitting to a specific area or viewpoint**: Physical construction, purpose of use, and other characteristics of cyber-physical system must be interpreted properly.

Ideas mentioned in Subsection 2.2 aim to solve these issues. “2-step risk evaluation” aims to solve Issue 2 and 3, and the combination of “asset container method” and “customized risk quantification method” aims to solve Issue 1 and 4.

Our goal in this paper is to focus on Issue 4 “fitting to a specific area or viewpoint” by customizing of vulnerability evaluation criteria and deepen our consideration. As an example of the issue, we conduct a case study to detect direct-access attacks in automobiles.

#### 3.2 Problem in Risk Evaluation of Direct Access Attacks

Direct-access attacks are defined as attacks where the attacker connects unauthorized equipment to an in-vehicle network directly. At first, direct-access attacks to automotive systems were considered unrealistic. Checkoway et al. mentioned that attackers with physical access could easily mount non-computerized attacks as well (e.g., cutting the brake lines) in their survey [26]. But many researchers have been studying a multitude of attack cases via in-vehicle network [27][28][29][30][31]. As mentioned in Section 1, direct-access attacks have become recognized as risks again, because there were some in car thefts [12].

Kawanishi et al. mentioned that direct-access attacks are no longer unrealistic because the attacker can attack more easily by such methods as renting a car through a car-sharing service and pretending to do maintenance [17]. At a factory, there are mechanisms to prevent direct-access attacks, such as setting a prohibited area requiring card authentication, but this is not the case with automobiles. The
direct-access attack to in-vehicle networks may have a higher risk than that in the factory. But in CRSS, the conventional risk quantification method, the risk scores of direct-access attacks are regarded as low.

3.3 New Approach to New Attacks and Merits

To detect new attacks such as direct-access attacks, we take a different approach. Since we want to guarantee the coverage of threats (Issue 1) as a methodology, it is desirable that the approach can also apply the asset container method. So we used a new quantification method RSS-CWSS_CPS. They confirmed that direct-access attacks on automotive systems were also as risky as other threats via network [17]. We promote RSS-CWSS_CPS instead of CRSS, a popular method. It is a risk quantification method applicable to the asset container method, and has the following two merits [18][25][32]:

A) CWSS attempts to use a more fine-grained metrics than CVSS for impact ratings (See C, I, A in Table 1 and TI, BI in Table 2). Indeed, TI and BI have seven ranks respectively, while each C, I, and A have only three ranks. There are 49 combinations of impact values for RSS-CWSS_CPS and only 27 combinations for CRSS.

B) CWSS has many similar metrics with CVSS suitable for asset container method, some of which may affect more finely evaluation than CVSS. Indeed, IC EC and EX in CWSS have ranks 8, 8 and 6 in order and the combination of attack complexity values is 384, while AC of CVSS has only three ranks.

4. Case Study of Risk Evaluation

Throughout the results of a case study in this section, we compare the difference of risk scores between RSS-CWSS_CPS and CRSS, and describe the usefulness of RSS-CWSS_CPS regarding Issue 4 “fitting to a specific area or viewpoint.”

In Subsection 4.1, we define an automotive system configuration model as the TOE. In Subsections 4.2 and 4.3, we introduce RSS-CWSS_CPS as a risk quantification method based on CWSS and show how to map the metrics and ranks. In Subsection 4.4, we consider advantages of RSS-CWSS_CPS for detecting direct-access attacks. In Subsection 4.5, we compare the results and see the differences of results between RSS-CWSS_CPS and CRSS. In Subsection 4.6, we compare the tendencies of the risk scores by entry points in each method. Finally in Subsection 4.7, we state the conclusions in the case study.

4.1 TOE Model

Liu et al. shows the network structure of a typical automotive system [33], and we used it as a TOE model (Fig. 1). In this TOE, functional modules for infotainment, telematics, and an ITS control console are connected via Ethernet network, and functional modules belonging to the control system of the power train (PT), body, chassis, advanced driver assistance system (ADAS), and immobilizer are connected via CAN bus network. A CGW (Central Gateway) also supports both networks. A thick black line is the boundary of the TOE, and the external square represents the equipment and environment outside the TOE. The small red and blue squares are the entry points to the TOE from the outside. Red squares are for normal entry points such as telecommunication or other media, and blue squares are for entry points for direct access, which are directly connected to the networks via the thick blue lines.

4.2 Risk Evaluation Method RSS-CWSS_CPS

RSS-CWSS_CPS is a risk quantification method based on CWSS which is defined in the ITU-T X.1525 standard [25]. Kawanishi et al. first applied CWSS to a data logger in an industrial control system as a TOE and confirmed that small equipment could be evaluated properly [16]. RSS-CWSS_CPS is a redefinition of the method in [16], and uses 8 of 16 metrics of CWSS. The risk score for a threat is calculated by the following equation (2) using CWSS...
metrics defined in Table 2:

\[ Rw = \text{SBase} \times \text{SSurface} \times \text{SEnv} / 10.0 \quad (2) \]

where

\[ f(x) = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{otherwise} \end{cases} \]

\[
\text{SBase} = \left\{ f(TI) \times (10TI + 15) \right\} \\
\text{SSurface} = \left\{ (20 \times (AV + 2) + 5 \times AS + 35) / 100.0 \right\} \\
\text{SEnv} = \left\{ 20 \times (AV + 2) + 5 \times AS + 35 \right\} / 20.0
\]

The formula of RSS-CWSS_CPS is the same one of CWSS whose unused metrics are set to “NA: Not applicable” (only metric IN is set to “A: Automated”). The eight CWSS metrics are used for the formula (2) because they are similar to CVSS metrics or more fine-grained to evaluate risks than CVSS ones. The only difference is the scale. The CWSS risk score takes a maximum of 100, while the CRSS risk score is a maximum of 10, so the risk score of the formula (2) is divided by 10 from the original CWSS equation to match the scale with CRSS.

4.3 Mapping of metrics in RSS-CWSS_CPS

According to the asset container method (see Subsection 2.2), CWSS metrics are assigned to the three perspectives, “where”, “at”, and “asset”, and the rank of each metric is determined. The metrics TI, BI, DI are assigned to “asset”. EC is assigned to “where”, and IC, AV, AS and EX are assigned to the combination of “where” and “at” which describes an attack path. Tables 3, 4, and 5 are excerpts of the actual data of these metrics in this case study.

4.4 Advantage of RSS-CWSS_CPS on Direct-Access Attacks

The advantage of direct-access attacks to in-vehicle networks is that “attackers can invade an in-vehicle network by relatively easy means such as renting a car and pretending to do maintenance to it.” RSS-CWSS_CPS is more advantageous than CRSS in interpreting this feature to solve the Issue 4 “fitting to a specific area or viewpoint.”

In judging attack feasibility, three metrics AV, Au and AC are affected by entry point and physical structure in CRSS, while five metrics AV, AS, IC, EC and EX are affected in RSS-CWSS_CPS. Table 6 shows CWSS metrics used in RSS-CWSS_CPS which can be influenced by the characteristics of the direct-access attacks. Especially, metrics IC and EC are originally internal and external mechanisms to mitigate the vulnerabilities of software. We interpret them as the hardware structure and physical boundary of the cyber-physical system and give flexibility to the interpretation of the system.

In addition to the difference in the number of metrics, weighting of these metrics in RSS-CWSS_CPS is also different from that in CRSS. Table 7 shows the amount of change in risk score when one metric is changed by 0.1 and all the remaining metrics are set to 1. The fluctuations by the metrics AV and Au in CRSS related to the entry point are 0.941, respectively, while those by the metrics AV and AS in RSS-CWSS_CPS are 0.2 and 0.05, whose fluctuations are as small as 1/4 or less. On the other hand, the fluctuation amount by the metric AC regarding the complexity of the attack of CRSS is 0.941, while the fluctuations amount by the metrics IC and EC of RSS-CWSS_CPS are both 1.0, which are higher than the fluctuation amount by CRSS. In this way, compared to CRSS, RSS-CWSS_CPS does not consider the difference of entry point as a decisive factor, but seems to require a comprehensive judgment involving other factors.

### Table 3: Mapping of TI, BI, and DI (excepted) [17].

<table>
<thead>
<tr>
<th>#</th>
<th>“At”</th>
<th>“Asset”</th>
<th>TI</th>
<th>BI</th>
<th>DI</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>CGW</td>
<td>Data Processing Function</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Diagnostic Function</td>
<td>M</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td>8</td>
<td>Telematics</td>
<td>Ex-Comm. Function</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Auth. Function</td>
<td>M</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Auth. Information</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote Service App.</td>
<td>M</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In-Comm. Function</td>
<td>M</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Personal Information</td>
<td>L</td>
<td>C</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Location Info / Status</td>
<td>L</td>
<td>M</td>
<td>M</td>
</tr>
</tbody>
</table>

### Table 4: Mapping of EC (excepted) [17].

<table>
<thead>
<tr>
<th>#</th>
<th>“Where”</th>
<th>EC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3G/LTE of Telematics</td>
<td>L</td>
</tr>
<tr>
<td>9</td>
<td>Direct-access via Ethernet</td>
<td>N</td>
</tr>
</tbody>
</table>

### Table 5: Mapping of IC, AV, AS, and EX (excepted) [17].

<table>
<thead>
<tr>
<th>#</th>
<th>“Where”</th>
<th>“At”</th>
<th>AV</th>
<th>AS</th>
<th>IC</th>
<th>EX</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Direct-access</td>
<td>CGW</td>
<td>L</td>
<td>N</td>
<td>N</td>
<td>H</td>
</tr>
<tr>
<td>17</td>
<td>via Ethernet</td>
<td>Telematics</td>
<td>L</td>
<td>N</td>
<td>N</td>
<td>H</td>
</tr>
<tr>
<td>24</td>
<td>3G/LTE of Telematics</td>
<td>CGW</td>
<td>I</td>
<td>M</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>26</td>
<td>Telematics</td>
<td>Telematics</td>
<td>I</td>
<td>M</td>
<td>N</td>
<td>H</td>
</tr>
</tbody>
</table>
4.5 Comparison of Result on Direct-Access Attacks

In Subsection 3.2, we mentioned that direct-access attacks have been regarded as unreasonably low risk compared to attacks via network. In the case study, we introduced RSS-CWSS_CPS to see whether this new method actually changes results.

We compare the risk scores of two threats and explain the difference in risk score of the direct-access attack due to the new quantification method. One of the two threats to be compared is #63 which is the threat to the external communication (Ex-Comm) function of the telematics module via telecommunication (3G/LTG) and the other is #208 which is the threat to the data processing function of the CGW module via direct-access.

Fig.2 is an enlarged view of the upper right part of the TOE model in Fig. 1 around the telematics module and the CGW module via direct-access.

Table 8 shows the comparison result between #63 and #208. The impact of each asset is defined by a set of metrics \{TI, BI, DI\} in RSS-CWSS_CPS, and \{C, I, A\} in CRSS. Regarding the impact of assets, the set of \{TI, BI, DI\} for both #63 and #208 is \{0.9, 0.9, 1.0\} in RSS-CWSS_CPS, and the set of \{C, I, A\} is \{0.00, 0.66, 0.66\} in CRSS. In terms of asset impact, there is no difference between the evaluation results of #63 and #208 in each of the evaluation criteria.

Differences between the risk scores are decided by other sets of metrics allocated by entry points and attack paths, that is “where” and “at” of the asset container method in Subsection 2.2. The corresponding set of metrics is \{IC, AV, AS, EX, EC\} in RSS-CWSS_CPS, and \{AV, AC, Au\} in CRSS.

AV in both criteria decides the advantage of the access vector (entry point) by the size of each value. The value 1.0 by #63 is larger than the value 0.5 by #208 in RSS-CWSS_CPS, and the value 1.0 by #63 is larger than the value 0.395 by #208 in CRSS, too. This means that the both criteria estimate that “#63 is riskier than #208 because #63 can be attacked via the network casually.”

AS in RSS-CWSS_CPS and Au in CRSS decide the advantage of authentication of the entry point by the size of each value. The value 0.8 by #63 is smaller than 1.0 by #208 in AS of RSS-CWSS_CPS, and the value 0.56 by #63 is smaller than 0.704 by #208 in Au of CRSS, too. This means that “#63 is less risky than #208 because of some authentication functions.”

The metrics that express the characteristics of the attack path is a set of metrics \{IC, EC, EX\} in RSS-CWSS_CPS and only AC in CRSS. In this case study, there is only the difference of EC in RSS-CWSS_CPS and AC in CRSS. EC in RSS-CWSS_CPS decides the weakness of the physical boundary by the size of each value, while AC in CRSS decide the complexity of the attack vaguely. The value 0.9 by #63 is smaller than 1.0 by #208 in EC of RSS-CWSS_CPS, and the value 0.61 by #63 is smaller than 0.71 by #208 in AC of CRSS, too. This means that “#63 is less risky than #208 because it is easy to connect to the in-vehicle network directly,” especially in RSS-CWSS_CPS, a more specific meaning of “by exploiting the vulnerability of the physical boundary” is added. In this way, the risk scores of these threats are calculated by both RSS-CWSS_CPS and CRSS. As a result of CRSS quantification, #63 (Rr = 7.95) was the highest risk threat of the total 494 threats of this automotive system, and #208 (Rr = 6.59) was the 23rd. On the other hand, as a result of RSS-CWSS_CPS, #63 (Rw = 8.13) was the 27th, and #208 (Rw = 8.21) was the 13th. Thus, the direct-access attack #208 has the disadvantage of having a lower value of the metric AV than that of the attack #63 via network, but it is not a decisive disadvantage in RSS-CWSS_CPS. Both threats are judged as significant.

From the viewpoint of the amount of change in Table 7 of Subsection 4.4, this result can be explained as follows:

- In CRSS, #208’s metric value compared to #63’s is 0.605 lower for AV, 0.144 higher for Au, and 0.1 higher for AC. By multiplying these differences by the amount of change for each metric and summing, we confirm that #208’s risk score is (0.605-0.144-0.1)·9.41=3.82 lower than #63’s.
- On the other hand, in RSS-CWSS_CPS, #208’s metric value compared to #63’s is 0.5 lower for AV, 0.2 higher for AS, and 0.1 higher for EC. By multiplying these differences by the amount of change for each metric
and summing them, we confirm that #208’s risk score is $-0.5 \cdot 2 + 0.2 \cdot 0.5 + 0.1 \cdot 10 = 0.1$ higher than #63’s.

- Thus, #208’s risk score is 0.1 higher than #63’s one in RSS-CWSS_CPS, while it is 3.82 lower in CRSS.

Actually, due to the interaction with other metrics, these values degenerate to 1.36 and 0.08 respectively, but we confirm the order reversal of #208 and #63.

The direct-access attacks are no longer unrealistic because the attacker can attack more easily by such methods as renting a car through a car-sharing service and pretending to do maintenance. Because of Merit B mentioned in Subsection 3.3 and the fact that the weighting for entry points is lighter as shown in Subsection 4.4 and Table 7, the risk quantification by RSS-CWSS_CPS seems to catch direct-access attacks well.

How to distinguish threats according to the risk score, such as prioritizing critical threats with high scores, will be controversial as a risk assessment methodology in future. However, RSS-CWSS_CPS has succeeded in widening the perception of security experts and making them pay attention to direct access. In fact, threats classified as moderate threats less than 7 points by CRSS are also judged as critical threats in RSS-CWSS_CPS. This result is an important achievement.

In this way, RSS-CWSS_CPS solves the Issue 4 “fitting to a specific area or viewpoint” in Subsection 3.1. Threat identification through metric interpretation can be achieved for the specific areas and perspectives.

4.6 Comparison of Priority on Entry Points

In this subsection, we compare which entry points tend to be considered risky by the two risk quantification methods. At first, we classified 11 entry points of the TOE into 4 categories for each communication distance:

- **Network (long distance):** 3G/LTE (Telematics module), and 3G/LTE (Infotainment module)
- **Adjacent (middle distance):** OTA (Power Train module), OTA (ITS module), and Bluetooth
- **Local (short distance with a simple interface):** OBD-II, Direct-access via CAN, and Direct-access via Ethernet
- **Other Local (short distance with a complicated interface to exploit):** USB, Power Line, and Sensor

We also compared threats with the highest rank in each category. Table 9 shows the result between RSS-CWSS_CPS and CRSS. In CRSS, the conventional method, the threat via “Network” was the 1st, “Adjacent” was the 11th, “Local” was the 23rd, and “Other Local” was the 125th. The four categories tended to be ranked in descending order of metric AV value of CRSS and in inverse proportion to distance. On the other hand, in RSS-CWSS_CPS, “Local” was the 1st, “Network” was the 27th, “Other Local” was the 45th, and “Adjacent” was the 78th. The order of the four categories was not necessarily the order of the largest metric AV values of RSS-CWSS_CPS or the order of inverse proportion to the distance.

This seemed to be due to the difference in evaluation between RSS-CWSS_CPS and CRSS. In RSS-CWSS_CPS, the distance of communication did not necessarily lead to an attack advantage, and other factors such as the need for authentication might work in the risk evaluation. As a result, “Adjacent” such as Bluetooth, which was farther than “Local” but required authentication, seemed to have lower risk than other categories.

4.7 Conclusion of Case Study

We confirmed that RSS-CWSS_CPS could detect direct-access attacks sensitively in addition to the threats detected by the conventional method. RSS-CWSS_CPS seems to be useful from the perspective of “fitting to a specific area or viewpoint” because it has two more metrics to interpret physical boundaries of cyber-physical systems.

We also compared the two risk quantification methods. CRSS tended to have a certain bias regarding the entry point, while RSS-CWSS_CPS didn’t have such a bias.

5. Discussion

This chapter summarizes what appears to be the benefits of applying CWSS to risk quantification methods in future studies for effective security design. We already mentioned the four issues to interpret effective security design procedure in Subsection 3.1.

5.1 Variance of Risk Scores Advantageous for 2-step Risk Evaluation

As a tendency of RSS-CWSS_CPS compared with CRSS, the distribution of the risk scores by RSS-CWSS_CPS is smoother than the distribution by CRSS risk scores. That trend seems to be prominent in the distribution of asset impacts. Fig.3 shows the difference between the histograms of risk scores when metrics not related to assets are regarded as constants. The peaks of the histogram of CRSS are very biased and scattered on the columns, while the histogram of RSS-CWSS_CPS is a gentle one close to the standard distribution. We think that this result is due to Merit A mentioned in Subsection 3.3, and that this tendency also affects the variance of the entire risk score.
5.2 Interpretation of Medium- to Long-Term Risks

In quantifying the risk associated with an attack, some risks are difficult to interpret properly. There is the risk of the attack itself, for example, “the risk that once the attack method is established and spread, the attack will be easier from the next time onward.” Such an examination is also a solution for Issue 4 “fitting to a specific area or viewpoint.” We expect that it is possible to interpret such “medium-to-long-term” risks by RSS-CWSS_CPS. The following four metrics in RSS-CWSS_CPS are considered to be able to differentiate the impact of the attack method itself to some extent.

- **TI**: TI is a metric that evaluates the technical impact of exploiting vulnerabilities, so it is possible to evaluate the magnitude of risk when attack methods become widespread.
- **BI**: BI is a metric that evaluates the impact on the current business and mission, so it can also evaluate the size of the cost for dealing with workarounds due to the spread of attack methods.
- **DI**: DI is a metric that evaluates the frequency with which vulnerabilities can be found, so it is possible to evaluate the improvement in attack ease when it becomes easier to find vulnerabilities to multi-stage attacks when attack methods become widespread.
- **EX**: EX is a metric that evaluates the frequency of exploitation of vulnerabilities, so it is possible to identify when the attack frequency increases as a result of the spread of attack methods.

In applying RSS-CWSS_CPS based on CWSS, considering the interpretation of these metrics will improve the accuracy and explanatory method for risk evaluation.

6. Conclusion

This paper presented four issues for security design procedure, and we focused on one of them, “fitting to a specific area or viewpoint.” As a solution, we mentioned the customization of a risk quantification method based on CWSS that is another approach to the conventional method based on CVSS v2, CRSS. RSS-CWSS_CPS customized from CWSS could explain all risks using only information via the attack victim and quantified the risk of cyber-physical systems through physical boundaries, especially the risk of direct-access attacks on automotive systems.

We conducted a case study of the risk evaluation of an automotive system focusing on detection of direct-access attacks. We confirmed that we could detect the direct-access attacks as risky as other critical threats detected by conventional methods. We also compared two methods and analyzed the differences between them.

RSS-CWSS_CPS seems to have appropriate number of metrics and ranks sufficient to quantify not only the characteristics of ICT systems but also the physical structure and boundaries of cyber-physical systems more flexibly.

References

KAWANISHI et al.: A STUDY OF THE RISK QUANTIFICATION METHOD OF CYBER-PHYSICAL SYSTEMS FOCUSING ON DIRECT-ACCESS ATTACKS TO IN-VEHICLE NETWORKS


Yasuyuki Kawanishi received the B.S. and M.S. degrees in Engineering from Tokyo University in 1991 and 1993, respectively. He is currently in both Sumitomo Electric Industries, Ltd., and National Institute of Advanced Industrial Science and Technology (AIST). He is also a doctor course student in Kyoto Sangyo University from 2021. His research interests include Cyber Security for the cyber-physical systems.

Hideaki Nishihara is a senior researcher at Cyber Physical Security Research Center of National Institute of Advanced Industrial Science and Technology (AIST). He has worked on formal approaches for system development for more than 15 years. His recent interests are in analyzing safety and security aspects of cyber-physical systems with formal models. He received his PhD degree from Osaka university in 2003.

HirotaKa Yoshida received the B.E. degree from Kobe University, Japan, in 1985, and the M.E. degree from Kyushu University, Japan, in 1987. Since 1987, he has been with the Sumitomo Electric Industries, Ltd. (SEI). His current research interests are in cyber security.

Hirotaka Yoshida received the B.S. degree from Meiji University, Japan, in 1999, the M.S. degree from Tokyo Institute of Technology, Japan, in 2001, and the Ph.D. degree in electrical engineering from KU Leuven, Belgium, in 2013. From 2001 to 2016, he was with the Research & Development Group, Hitachi, Ltd. He is currently a team leader at the National Institute of Advanced Industrial Science and Technology (AIST). He is a member of IACR, IPSJ, and JSAE. In 2013, he won the award of industrial standardization that has been granted by the Japanese Ministry of Economy, Trade and Industry (METI).

HiroYuki Inoue received the B.S. and M.S. degrees in electronic engineering from Osaka University in 1987 and 1989 respectively, and received the Ph.D. degree in engineering from the Nara Institute of Science and Technology in 2000. He has been a Professor with the Faculty of information Science and Engineering, Kyoto Sangyo University, since 2021. He is also a visiting researcher of AIST. His research interests include technologies for embedded security, especially automotive network security, and network protocol of the Internet.