J Ambient Intell Human Comput (2018) 9:531–551
DOI 10.1007/s12652-016-0442-8

ORIGINAL RESEARCH

Security risk assessment framework for smart car using the attack tree analysis

Hee-Kyung Kong[1] · Myoung Ki Hong[2] · Tae-Sung Kim[3]

Received: 1 October 2016 / Accepted: 26 December 2016 / Published online: 27 January 2017

Abstract As the automobile industry has recently adopted information technologies, the latter are being used to replace mechanical systems with electronically-controlled systems. Moreover, automobiles are evolving into smart cars or connected cars as they are connected to various IT devices and networks such as VANET (Vehicular Ad hoc NETwork). Although there were no concerns about the hacking of automobiles in the past, various security threats are now emerging as electronic systems are gradually filling up the interiors of many automobiles, which are in turn being connected to external networks. As such, researchers have begun studying smart car security, leading to the disclosure of security threats through the testing or development of various automobile security technologies. However, the security threats facing smart cars do not occur frequently and, practically speaking, it is unrealistic to attempt to cope with every possible security threat when considering such factors as performance, compatibility, and so forth. Moreover, the excessive application of security technology will increase the overall vehicle cost and lower the effectiveness of investment. Therefore, smart car security risks should be assessed and prioritized to establish efficient security measures. To that end, this study constructed a security risk assessment framework in a bid to establish efficient measures for smart car security. The proposed security risk assessment framework configured the assessment procedure based on the conventional security risk analysis model GMITS (ISO13335) and utilized 'attack tree analysis' to assess the threats and vulnerabilities. The security risk assessment framework used the results of an asset analysis, threat/vulnerability analysis, and risk analysis to finally assess the risk and identify the risk rating. Moreover, it actually applied the proposed framework to assess security risks concerning targeted increases in vehicle velocity and leakages of personal information, which are the leading threats faced by smart cars. Here, the framework was applied to vehicle velocity increase and personal information leakage, which are the leading threats.

Keywords Security risk · Assessment framework · Vulnerability · Smart car · Attack tree analysis

1 Introduction

As automobile parts are being transformed into ECUs (Electronic Control Unit), the convenience and safety of automobiles have improved, while the increasing use of electronic parts means that there are more elements of ICT (Information and Communication Technology) inside automobiles. The advance of ICT has not only enabled automobiles to communicate with external networks through such technologies as V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure), but has also facilitated wireless network communications such as Bluetooth and Wi-Fi. A smart car is defined as a vehicle whose information system is managed and supported through both internal and external networks (Han 2012). Experts estimate the size of the world

✉ Tae-Sung Kim
kimts@cbnu.ac.kr

[1] Department of Information and Communication Engineering, Chungbuk National University, 1 Chungdae-ro, Seowon-gu, Cheongju, Chungbuk 362-763, South Korea

[2] Department of Information Security Management, Chungbuk National University, 1 Chungdae-ro, Seowon-gu, Cheongju, Chungbuk 362-763, South Korea

[3] Department of Management Information Systems, Chungbuk National University, 1 Chungdae-ro, Seowon-gu, Cheongju, Chungbuk 362–763, South Korea

smart car market to be around 230 trillion Korean won, and predict that it will be growing at an average annual rate of 6.7% by 2018 (KDB Research 2014). However, the amount of ICT installed in automobiles is also increasing the possibility of hacking attacks against automobiles. The Automobile Security Research Center of Korea University conducted a hacking test with automobiles and succeeded in operating steering wheels and increasing the engine's velocity using a mobile phone (Cho et al. 2012); and some other automobile hacking tests were conducted in other countries even earlier (Miller and Valasek 2013; Koscher et al. 2010). Recognizing the seriousness of the problem, countries such as the US, the EU and Japan are conducting national projects to reduce automobile security risks. Automobile hacking is considered more serious than other forms of hacking because it can threaten the driver's and passenger's life, given that automobiles are becoming more dependent on electronics and networks. Security experts already recognize an automobile as a computer on wheels, as the virus and hacking techniques deployed within the conventional ICT environment are now beginning to target automobiles. Although it is recognized that security threats against automobiles are increasing, it is unrealistic to try to cope with every possible security threat when considering such factors as efficiency and cost. As security threats to automobiles do not occur often as yet, adopting every available security solution only serves to increase the overall cost of a vehicle, making the security solution inefficient in terms of effectiveness of investment. The Control System Security Research Group of the National Institute of Advanced Industrial Science and Technology (AIST) in Japan argued that adopting all security measures against automobile hacking is unrealistic when considering compatibility and cost, and suggested countermeasures to automobile hacking based on the risk management methodology. Moreover, Wolf and Scheibel (2012) argued for a methodology and assessment based on systematic risk analysis, since it is difficult to apply security solutions and their excessive application will only result in a waste of money. For risk management-based measures, the threats to and vulnerabilities of smart cars must be identified and analyzed, and a security risk assessment must be performed first. Therefore, this study intends to propose a security risk assessment framework with a view to establishing efficient security measures for smart cars. The main objectives of this study are, first, to propose a systematic security risk assessment framework based on risk management to establish the efficient security measures of smart cars; second, to apply the framework to identify and categorize the assets, threats and vulnerabilities of smart cars; and, third, to analyze the results of identification and categorization in order to deduce the risk rating of the threats and vulnerabilities of each asset.

2 Theoretical background

2.1 Literature on smart car security

2.1.1 Concept of the smart car

Recently, more and more mechanical automobile parts have been replaced by electronic parts. This is largely because the ECU enables the precise measurement of automobile operation and a quick response to safety incidents. For that reason, the number of ECUs mounted in an automobile is increasing. In the case of a single cutting-edge car, there may be 145 or more actuators, 4000 or more signal data, and 75 or more sensors (radar, sonar, camera, acceleration gauge, thermometer, rainfall sensor, etc.). It has been reported that these instruments generate more than 25 GB data per hour and are analyzed by 70 or more OBC (Onboard Computer) (Kim and Lee 2014). As ever more ECUs are mounted in a vehicle, it becomes connected to more external networks for communications between vehicles and for communications between a vehicle and a device. Due to the rising use of external networks, conventional cars are being replaced with connected cars and smart cars. A smart car is a car that integrates in-vehicle information to improve safety and convenience as well as to provide useful information (Han 2012). In the USA and Europe, a smart car is defined as a self-driving car (otherwise known as the driverless, robotic or autonomous car) or a connected car, and is considered an integral part of the ITS (Intelligent Transport System) (Han 2012). In South Korea, a smart car is considered a step toward the self-driving car; and it is expected smart cars will be replaced by self-driving cars in the not-too-distant future. Regarding internal and external vehicular communication, wired and wireless communication technologies such as Bluetooth, Wi-fi, RFID, DSRC (Dedicated Short Range Communications), NFC (Near Field Communication), GSM (Global System for Mobile Communications), CDMA (Code Division Multiple Access) and UMTS (Universal Mobile Telecommunication System), all of which are widely distributed in existing IT areas, have already been applied to cars (Kim and Lee 2014). A smart car is fitted with many ECU parts which are connected through an internal network for the exchange of data. VANET (Vehicle Ad hoc Network) enables the exchange of accident data and traffic data between the ITS and vehicles, and the exchange of data between vehicles. An ECU controls the operation of various automobile units such as the engine, automatic transmission and ABS (Anti-Lock Braking System) with a computer (Cho et al. 2012). Although the ECU was initially developed to improve fuel efficiency by precisely controlling ignition timing and fuel injection, its application has been gradually expanded to other parts and modules.

2.1.2 *Smart car security*

In recognition of the security risks facing smart cars, various studies on automobile security measures have been ongoing. Such studies focus mostly on experiments concerning the possibility of car hacking, and there are also various technological studies related to the ITS such as the development of an encryption module for in-vehicle network communication and a security module for ECUs. There have also been many recent managerial studies on automobile security to identify and categorize the security vulnerabilities and risks disclosed in technical studies on automobile security. Table 1 summarizes the preceding studies on smart car security.

The relevant technological studies can be mainly divided into four categories: VANET, ECU/CAN network, SW/HW, and other vehicle systems. In one of the VANET-related technological researches, Lim (2011) pointed out the problem of inefficiency due to the lack of communication ability of the RSU (Road Side Unit) and personal information leakage from the RSU in VANET communication, and then proposed a group signature-based protocol model focusing on authentication to prevent information leakage. Patsakis et al. (2014) analyzes current practices and standards of the automotive industry, highlighting several vulnerabilities that stress the need to change the way that in-vehicle communication is handled. Raya and Hubaux (2007) studied the implementation of encryption in the VANET network and presented a security mechanism for VANET by encryption of the data based on the key management, authentication, and signature of the network data. As for ECU/CAN network-related technological researches, Cho et al. (2012) conducted automobile hacking experiments and, recognizing the problem whereby data are not encrypted in the CAN network, proposed a message authentication and allocation mechanism for the CAN network. Koscher et al. (2010) conducted the first study on hacking through the CAN network and the ECU in automobiles and demonstrated the hacking of automobiles using Carshark, which is an SW for automobile hacking. Kim et al. (2013) implemented secure diagnostics using an encryption mechanism and a random number generator. This was implemented with a diagnosis tool and authentication communication between the ECUs; and could protect communications from arbitrary data manipulation, DDoS commands, and wiretapping. As for HW/SW-related technological studies, Nilsson and Larson (2008) pointed out the problems surrounding the wireless updating of ECU firmware in smart cars and proposed SFOTA, a security firmware update protocol model. Hossain and Mahmud (2007) presented security measures for wireless software upload from a vehicle and verified, using the simulation result, that security could be improved by transferring the packets with a multi-copy method instead of a single-copy method during wireless software upload. Wolf and Gendrullis (2011) designed, implemented and evaluated a hardware security module for automobiles. For communications between automobiles or between ECUs, such requirements as key storage and a crypto engine were identified, and a hardware security module was designed and implemented according to those requirements. Rouf el al. (2010) experimentally demonstrated that data can be manipulated or

Table 1 Literature on smart car security

		Research subject	References
Security technology	VANET	Security mechanism implementation Encryption implementation	Lim et al. (2011) Raya and Hubaux (2007)
	ECU/CAN network	Hacking test using ECU and CAN ECU communication security implementation Network message authentication	Kim et al. (2013) Koscher et al. (2010) Cho et al. (2012)
	SW/HW	Firmware update security SW upload security Security module development	Wolf and Gendrullis (2011), Hossain and Mahmud (2007) Nilsson and Larson (2008)
	Other vehicle systems	TPMS (Tire Pressure Management System) PKES (Passive Keyless and Entry System)	Francillon et al. (2011) Rouf et al. (2010)
Security management	Risk identification and categorization	Risk categorization based on vehicle network Risk categorization using the CETR's attack categories Risk categorization based on a hacking scenario	Studnia et al. (2013) Brooks et al. (2009) Checkoway et al. (2011)
	Security assessment method	Study on an assessment method using the automobile engineering standard VANET security risk assessment	Wolf and Scheibel (2012) Ren et al. (2011)

wiretapped using the local area network, since the TPMS (Tire Pressure Management System) transfers data through the wireless local area network. Francillon et al. (2011) reported the first hacking experiment of the PKES (Passive Keyless and Entry System) and presented countermeasures to such hacking. The study executed a relay attack based on the fact that the vehicle and the key communicate remotely. As for smart car managerial studies, Studnia et al. (2013) categorized and analyzed automobile hacking not from the technological perspective but from the managerial perspective, i.e., the purpose and origin of the attack. The study identified and analyzed the risk possibility of automobile hacking—such as internal attack, remote attach, direct approach, and physical approach centered on external networks—and presented a protection mechanism based upon it. Brooks et al. (2009) categorized automobile hacking into anti-theft system, VANET, ECU flashing, and integration of business service based on the CERT's categorization of attacks. The categories were further segmented into attack, vulnerability, target, and result in order to analyze the level of hacking risk. Even the various external stakeholders such as automobile manufacturers and vendors were identified using the usecase. Checkoway et al. (2011) experimentally analyzed the attacks against automobiles, and then categorized and evaluated their vulnerabilities. Using scenarios, the vulnerabilities were categorized into the following three types: indirect physical access, short-range wireless access, and long-range wireless access. Wolf and Scheibel (2012) analyzed the security risks of automobiles and proposed a security risk assessment framework based on the following formula: risk = probability of an accident × expected losses through that accident. The framework was organized in such a way that the security risks were quantitatively assessed by experts based on the SIL (safety integrity levels) analysis and the CEM (Common Evaluation Methodology) analysis. Ren et al. (2011) conducted an assessment of the security risks of VANET. A model was developing using the attack tree technique, and the risk assessment was conducted with the probability drawn from the cost, technical difficulty, and possibility of occurrence between the nodes.

Automobile security-related projects are ongoing in many countries (Bharadiya et al. 2014), usually with the focus on smart cars linked with the ITS rather than on vehicles themselves. In the US, security projects are mainly led by government agencies such as the SAE (Society of Automotive Engineers) and the Safety Pilot project of the US Department of Transport. In February 2011, the SAE formed a security-related committee called TEVEE18, which reviews methods of detecting and dealing with intrusions into automobile electronic systems and minimizing damages even after intrusion. The Safety Pilot project conducted by the US Department of Transport field tests communications between vehicles, with the focus primarily on V2V and V2I, i.e., communication between vehicles and communication between vehicle and cutting-edge transportation system, respectively. It also evaluates the security and protection of personal information. Since the project deals with communication between vehicle and cutting-edge transportation system, it also covers security of communication between vehicles and between ITS and vehicle. In addition, the SEA and US Department of Transport are studying threat evaluation techniques and the related requirements by reviewing the NIST SP800-53 and STRIDE threat modeling techniques from Microsoft, as well as the security of ECUs (Kim and Lee 2014). In Europe, automobile manufacturers have formed consortiums to carry out various security-related projects including EVITA (E-safety Vehicle Intrusion proTected Applications), PRESERVE (Preparing Secure Vehicle-to-X Communication Systems), and OVERSEE (Open Vehicular Secure Platform). There are also projects that are being carried out by academic societies and other bodies. As in the US, these projects are mostly derived from studies of cutting-edge transportation systems, and focus on security issues concerning communications between ITS and vehicles. In Japan, automobile security projects are mostly led by the JSAE (Society of Automotive Engineers of Japan) and JEITA (Japan Electronics and Information Technology Industries Association). The standardization of automobile security is the leading example of research subjects. As in Europe, the forming of automobile security-related workshops and academic societies has stimulated considerable interest in security.

However, the preceding studies of smart cars fell short of actually measuring and assessing the risks of the vulnerabilities or threats that had previously been identified and categorized concerning smart cars, although they were significant in that they established technological measures through hacking tests and encryption implementation. Moreover, there was a shortage of studies on how to manage the security threats to smart cars and on which methodology should be used for assessment in order to establish efficient security measures. It would be inefficient and would increase the overall cost of a vehicle if it were to be installed with every possible security solution. Although concern about automobile security is serious enough since an accident can threaten human life, such security incidents rarely occur at present, and there have been few cases of hacking to date. In that respect, what is needed is an assessment of the potential risks based on an analysis of the security risks facing smart cars, in order to selectively establish effective security measures. Wolf and Scheibel (2012) argued for a methodology and an assessment of risk analysis since it was difficult to actually apply security solutions, and because the excessive application thereof can result in a waste of money. Therefore, studies on methodology and modeling are necessary to establish efficient security measures by identifying and categorizing the assets, threats and vulnerabilities through the security risk assessment of smart cars, and by using the risk assessment deduced from the results of analysis. Just as other industries analyzed and assessed the risks in order to establish security measures from the information protection viewpoint as a result of the widespread application of ICT (Petrlic et al. 2013; Viduto et al. 2011), so the smart car industry will also need to commission studies aimed at establishing efficient security measures by analyzing and assessing the security risks arising from the adoption of ICT. As such, this study developed a security risk assessment framework based on the conventional security risk analysis model GMITS (ISO13335) in an attempt to analyze and assess the risks from the information protection viewpoint, and utilized the 'attack tree' analysis to analyze the threats and vulnerabilities.

2.2 Literature on security risk assessment

2.2.1 Security risk assessment

As security risk analysis is the key part of the risk management process (Cha and Kim 2013), various models have been devised to analyze the risks (Bernardo and Hoang 2012). This study describes the risk analysis model based on GMITS (ISO13335) and SP 800-30 devised by NIST (National Institute of Standards and Technology), which are currently the leading standard models of security risk analysis. GMITS (Guidelines for the Management of IT Security), also called ISO/IEC13335, is the standard technology report issued by ISO/IEC JTC 27, which is a joint technical committee. It is composed of the following five parts; (Part 1) IT Security Concept and Model; (Part 2) Management and Planning; (Part 3) Management Technique; (Part 4) Countermeasures; and (Part 5) Network Connection Guideline (ISO/IEC 1998). Parts 2 and 3 describe the risk analysis process and detailed risk analysis/assessment methodology. Standards such as ISO27001 and BS15000 recommend conformance to this technique and process. GMITS (ISO13335) presents a detailed risk management analysis, assessment process, and assessment method. The security risk management is described in terms of the proportional relationship of assets, threats and vulnerabilities. Calculation of the level of risk is shown in Eq. (1). In the equation, R represents the risk, A the assets, T the threat, and V the vulnerability. The proportional relations defined in Eq. (1) relatively change according to the risk management criteria of each organization (Kim et al. 2008).

$$R = A \times T \times V. \tag{1}$$

The risk analysis procedure involves asset analysis, threat analysis, and vulnerability analysis. The risk analysis assesses the level of risk using the results of the asset, threat and vulnerability analyses. First, the asset analysis defines and categorizes the asset, then prioritizes the assets according to their importance. Second, the threat analysis identifies and categorizes the threats, then calculates the frequency of the threats and the probability of their occurrence. Third, the vulnerability analysis analyzes the actual problems that may lead to security incidents such as the hacking of information assets. Fourth, the degree of risk is assessed using the risk level formula "$R = A \times T \times V$" based on the result of the risk analysis. Last, the DoA (Degree of Assurance), which defines whether the risks that remain after the risks identified by the risk analysis have been removed, mitigated, accepted or transferred are acceptable, is assessed. The US-based NIST announced "FIPS PUB (Federal Information Processing Standards Publication) 65: Risk Analysis Guidelines on Automobile Information Processing" in order to present a model for basic risk management and analysis (NIST 2002). It also announced SP 800-30 (Risk Management Guide for Information Technology Systems) to lay the groundwork for security risk analysis. The NIST model allows users to select an analysis technology to perform the security risk analysis in accordance with the organizational environment. The analysis technique can be freely selected, and the target and depth of the analysis can be determined in accordance with the selected analysis technique.

2.2.2 Security risk assessment in each industry

Different industries have been using different methods of assessing security risks. This section describes studies that used the security risk assessment methodology to analyze the security risks of smart grids. Kang et al. (2013) proposed a quantitative analysis of the security risk of SCADA, which controls numerous power systems. Ray et al. (2010) proposed an integrated approach framework to managing the risks faced by smart grid systems by conducting a risk assessment based on impact and priority after categorizing the threats and vulnerabilities. Ko et al. (2013) suggested a network model of the AMI (Advanced Metering Infrastructure) to assess the security threats to smart grids and generated various attack scenarios. They utilized the attack graph as a technique for quantifying the security vulnerabilities of SCADA systems. Hahn and Govindarasu (2011) proposed a framework to assess the level of exposure to attack facing smart grid systems. They identified the cyber risks based on the risk assessment procedure and developed the corresponding exposure graph; and verified the framework using virtual simulation. Security risk assessments of nuclear power generation systems are also ongoing. Kang and

Jeong (2010) pointed to the increasing likelihood of security risks due to the widespread adoption of ICT in nuclear power instrument control systems, and proposed a method of assessing cyber security risks for nuclear power instrument control systems based on the conventional information security risk assessment. Chen et al. (2009) conducted a network risk assessment of nuclear power generation systems, presenting 14 managed items using the OCTAVE methodology based on the attack scenarios.

2.2.3 *Security risk assessment using attack tree*

The attack tree first proposed by Weiss (1991) is useful in identifying threats and vulnerabilities by using modeling. It expresses all possible attack elements and provides both a logical approach and a visual means of identifying the threats and vulnerabilities by determining which event must be generated for an attack to be successful. Schneier (1999) proved that the attack tree was very useful in identifying attack possibilities and threats by identifying the threats and risks in greater detail (Pudar et al. 2009). A tree structure is composed of a root node, which represents the final goal of an attack, and the intermediate nodes, which represent the various attack methods used to achieve a given goal. Existing tree analysis techniques such as ETA (event tree analysis) and FTA (fault tree analysis) generally generate scenarios for a specific virtual incident and analyze them to measure the risks entailed by a specific incident. An attack tree is also a quantitative and qualitative assessment technique that can be used for logical and structural analysis of system attacks in the information security area. For that reason, it is widely used to logically model cyber-attacks against major national infrastructures such as power plants, nuclear power stations, and the defense industry (Uhm 2012).

An attack tree consists of a root node, which represents the final goal of an attack, and child nodes in ‘OR’ or ‘AND’ conditions. An OR node means that a given incident is possible if any other nodes are true, while an AND node requires all other nodes to be true. When an attack tree is designed, a value is assigned to each of the intermediate nodes, and the value of each node is calculated. Security measures are then established in accordance with those values (Uhm 2012). An attack tree is composed of a vertex (v), edge (ε) and set (θ), as shown in Fig. 1, and is expressed as Attack Tree = (v, ε, θ) (Uhm 2012).

- V is the highest root node of the tree and represents the final goal of an attacker. V is separated into the leaf_nodes and internal_nodes. A leaf_node is the node in the lowest level, like V_4 in Fig. 1, and is not connected in a set with other child nodes. An internal_node is an intermediate node like V_1 and is connected with other nodes in sets.
- Set = [AND, OR]
- If a node V ∈ internal_node and all edges connected to the node are connected in the AND condition, it is defined as an AND set. All internal_nodes connected in the AND condition must perform the attack event.
- If a node V ∈ internal_node and all edges connected to the node are connected in the OR condition, it is defined as an OR set. Only one of the internal_nodes connected in the OR condition needs to perform the attack event.

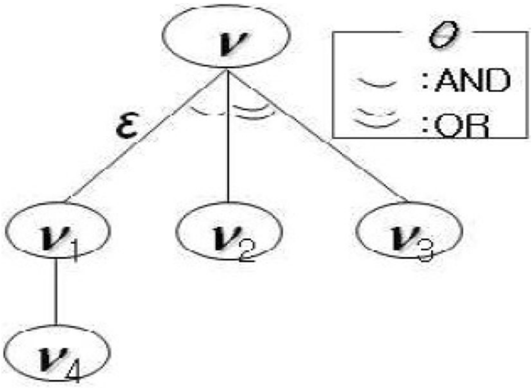

Fig. 1 Configuration of attack tree

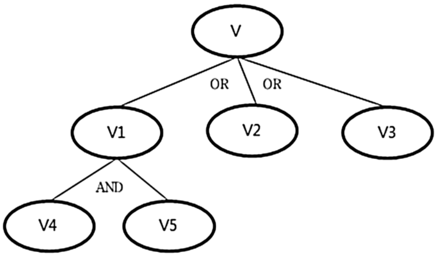

Fig. 2 Example of the calculation of threat assessment value using an attack tree

Use of attack tree to calculate the probability of occurrence of attacks using the attack tree Ketel (2008) calculated the risks using the probability formula of the child node structure of ‘AND or OR’. Uhm (2012) proposed methods of measuring threats using attack trees, and reported that an attack tree analysis can be used to predict the scenarios of system attacks, and thus can calculate the probability of an attack and the threat indices.

Figure 2 shows an example of the calculation of threat assessment value using an attack tree. In the circuit theory, a resistance value is defined as the value that restricts the flow of a current. When such a resistance formula is applied to an attack tree, the value that can delay the generation of an attack from the lowest level node to the top node can be obtained. Since the resistance value reduces the threat, the reverse value of the resistance value can represent the degree of threat. The threat assessment formula is shown below equations 2 and 3 (Uhm 2012; Ketel 2008).

$$\text{AND set: } 1 - (\text{V1} + \text{V2} + \text{V3}), \tag{2}$$

$$\text{OR set: } 1 - (\text{V1} \times \text{V2} \times \text{V3})/((\text{V1} \times \text{V2}) + (\text{V2} \times \text{V3}) + (\text{V3} \times \text{V1})). \tag{3}$$

Each node (V) reflects the event by the probability formula, and the final root node contains the event values generated by the nodes from bottom to top.

An attack tree can also calculate the probability of occurrence of an attack through modeling (Ketel 2008; Uhm 2012). Uhm (2012) pointed out that the probability of occurrence of attacks meant the ratio of occurrence of attack events in all child nodes to all attack nodes related to the parent node in order to accomplish the goal of the attack in the parent node. In other words, the probability of occurrence of attacks is obtained from the number of sets and child nodes of a parent node. Equations 4, 5 and 6 show the formula for the probability of occurrence of attacks.

$$\begin{aligned}&\text{In the case of a single node, the probability}\\ &\quad\text{of occurrence of attacks} = 1,\end{aligned} \tag{4}$$

$$\begin{aligned}&\text{In the case of the AND set, the probability of occurrence}\\ &\quad\text{of attacks} = \text{Number of AND cases/total number}\\ &\quad\text{of nodes,}\end{aligned} \tag{5}$$

$$\begin{aligned}&\text{In the case of the OR set, the probability of occurrence of}\\ &\quad\text{attacks} = 1/\text{Total number of nodes.}\end{aligned} \tag{6}$$

Utilization of attack tree analysis Table 2 shows literature on attack tree analysis is widely used in analyzing security threats and vulnerabilities in infrastructure industries such as defense, SCADA systems, and the smart grid (Uhm 2012). In the infrastructure industry, a security incident can cause great loss and damage, but the intrusion frequency and occurrence rate are not very high, making it difficult to assess threats and vulnerabilities as the amount of existing data is small. The attack tree is widely used for the analysis of security risks in the infrastructure industry as it can estimate threats and vulnerabilities between nodes using the probability formula based on attack scenarios even when the intrusion frequency and occurrence rate are low or when there is only a small body of existing data related to security incidents. Moreover, it can show a logical model for threats of and vulnerabilities to system attacks by visual means. The smart car industry is similar to the infrastructure industries in that it is difficult to assess any threats and vulnerabilities because there have been few cases of security incidents to date. As such, this study identified and modeled the security threats to and vulnerabilities of smart cars and assessed them using the probability formulas.

3 Smart car security risk assessment framework

The security risk assessment and attack tree analysis were theoretically described, and the need for security risk assessment was presented by analyzing the significance and limitations of preceding studies on automobile security. To assess the security risks facing smart cars, a comprehensive analysis of assets, threats and vulnerabilities is needed. The framework proposed in this study also analyzes the risks based on an analysis of assets, threats and vulnerabilities. This section introduces the smart automobile security risk assessment procedure proposed in this study and compares it with the automobile security risk assessment procedure proposed by Wolf and Scheibel (2012).

3.1 Smart automobile security risk assessment procedure

The smart automobile security risk assessment framework proposed by this study is essentially based on the security risk analysis model specified by GMITS (ISO13335), and the attack tree analysis method is used to analyze threats

Table 2 Literature on attack tree analysis

Type			Research	References
Attack tree	Methodology		Development of assessment method ACT (attack countermeasure tree)	Uhm (2012), Ketel (2008) Lv and Li (2011) Roy et al. (2010) Pudar et al. (2009)
	Security research	Industrial system	SCADA system security research Smart grid security research VANET security assessment	Wi et al. (2013) Kim, et al. (2011) Li et al. (2010) Ren et al. (2011) Ten et al. (2007)

and vulnerabilities. The threats to and assets and vulnerabilities of smart cars must be clearly defined before the security risk assessment, but few studies have clearly defined their assets, threats and vulnerabilities. Therefore, this study defines the threats to and assets and vulnerabilities of smart cars based on the definition provided by GMITS (ISO13335) and the EVITA project. The procedure for assessing the security risks of smart cars is described as follows:

3.1.1 Asset analysis

Asset analysis is the procedure by which the assets of smart cars are defined, identified and categorized in order to evaluate the importance of each asset. To that end, it uses the severity evaluation technique of the EVITA project and configures the importance evaluation items.

Asset identification and categorization An 'asset' is a target to be protected and includes the information, documents, manpower, HW and SW of an organization. The EVITA project specified a total of 16 assets including the chassis safety controller, powertrain controller, and wireless communications of a smart car (EVITA 2009). This study defined the assets based on which systems should be protected when a vehicle is attacked by a hacker. Of the many ECUs installed inside a car, the assets were specified in the major category based on module production, which is the divide-and-conquer method (EVITA 2009). This study categorizes various subsystems such as the powertrain, chassis, body, and infotainment as the assets of a smart car.

Assessment of importance of assets The importance of an asset is measured in terms of the loss that can occur at the time of an intrusion incident. However, it is difficult to measure the importance from a uniform viewpoint in the case of an automobile. That is because an automobile incident not only results in property loss but also affects human life and vehicle operation. Therefore, this study configured the importance evaluation items based on the severity evaluation items of the EVITA project. The items will be evaluated with the three items of 'safety', 'privacy', and 'operational', excluding the financial item from the four items used to evaluate severity in the EVITA project. In the EVITA project, the financial item includes the financial damages sustained by various stakeholders, such as the losses of automobile manufacturers. However, as the scope of this study did not include the financial damages of stakeholders such as automobile manufacturers, the financial items were excluded. The scale of each measured value was 1–3. Table 3 shows the asset importance evaluation items.

- *Safety* Level of safety that can affect the driver's life;
- *Privacy* Level of access to or tracking of the vehicle or driver information; and
- *Operational* Level of impact on the system and its functions without affecting safety.

3.1.2 Threat/vulnerability analysis

Kang et al. (2013) pointed out that the level of a threat and whether that threat materializes or not were related to the vulnerability of the system and that, if a threat was an exogenous variable, a specific vulnerability was an endogenous variable of the system. An attack tree is modeled with the attack scenarios. Such a model can assess threats and vulnerabilities through the probability formula by figuring out the relationship between the various threats and vulnerabilities.

Identification of threats A threat is a source of a risk that can negatively affect an asset using the vulnerability of the asset, or an external environment of an event that can negatively affect the security of an information asset considering the purpose of the IT service (Narita et al. 2013). A threat can be an earthquake, flood, virus infection or illegal access. This study defined a threat as the purpose of a hacker's attack. In other words, a threat is the ultimate goal of an attack, such as the stopping of a vehicle engine or the theft of personal information from a car, which the hacker intends to accomplish by hacking a smart car system.

Identification of vulnerabilities Vulnerability refers to a lack of measures to prevent the weakness or threat inherent to an asset. For example, it includes a password that can be easily inferred, potential enables the remote accessing of root, or the lack of a security patch. This study defined the threats based on which path a hacker takes to intrude into an internal system of a vehicle or which attributes or functions the hacker uses to intrude into the system.

Table 3 Asset importance evaluation items

class	Safety	Privacy	Operational
1	No damage	Unauthorized access without data	No problem with operating the vehicle
2	Light injury	Unauthorized access to only anonymous data	A problem that can be recognized and identified by the driver (No problem with operating the vehicle)
3	Serious injury or life-threatening injury	Unauthorized access to data that can identify or track the vehicle or driver	Significant impact on vehicle performance (Great impact on vehicle operation)

Attack tree modeling An attack tree is modeled using the threats and vulnerabilities that have been identified and categorized. In an attack scenario, a root tree becomes the purpose of an attack, i.e., a threat, and the bottom nodes become the vulnerabilities. Figure 3 shows an attack tree modeling for threat/vulnerabilities analysis of the smart car.

Assessment of threats After the attack tree modeling, a threat evaluation is performed. A threat is evaluated using the equations 2 and 3, and the security threat to a smart car is evaluated using the attack tree risk evaluation method described in Theoretical Background (Ketel 2008; Uhm 2012). A threat is expressed as T, and the range of measurement is 0.0–1.0.

Assessment of vulnerabilities A vulnerability evaluation is a series of processes designed to identify the vulnerabilities of information system assets and analyze the path (vulnerability) used by an attack to intrude upon the assets in order to threaten them, and then to quantify the measurement. Kang et al. (2013) pointed out that vulnerability can be regarded as the probability of a threat to an information asset being materialized, and that it has the value of $0 \leq V \leq 1$, where the vulnerability is 1 when the threat is completely passed through information system assets, and is 0 when no threat is passed through them. In other words, the vulnerability can be quantified in a probability term expressing its relationship with a given threat. It represents whether a threat can intrude upon the information asset through the vulnerability, and can be quantified using the probability of success and failure if the past data are insufficient (Kang et al. 2013). The vulnerabilities can be evaluated using the probability values calculated by the attack tree model. The possibility of success in each node of the tree model is set at 0.5(1/2) to evaluate the vulnerability. However, it would be difficult to properly evaluate the vulnerability using such a simple probability. Therefore, this study measured the vulnerability using the probability of the vulnerability and events in the same way as the threat evaluation, and then evaluated the vulnerability by reflecting the probability of intrusion success during an event. The following Eqs. 7and 8 are used to calculate the vulnerability level using the attack tree:

$$\text{In the case of an AND set: (V1} \times \text{success probability (1/2))} + \text{V2}, \tag{7}$$

$$\text{In the case of an OR set: ((V1} \times \text{success probability (1/2))} \times \text{V2)/((V1} \times \text{success probability (1/2))} + \text{V2)}. \tag{8}$$

The threat began at 0 and gradually increased, while the vulnerability began at 1 and gradually decreased. The intrusion possibility, i.e., the possibility of success or occurrence, of a threat applied through a vulnerability gradually decreased from the bottom node to the top node, because the intrusion possibility decreases as the number of nodes gradually increases during the execution of the attack.

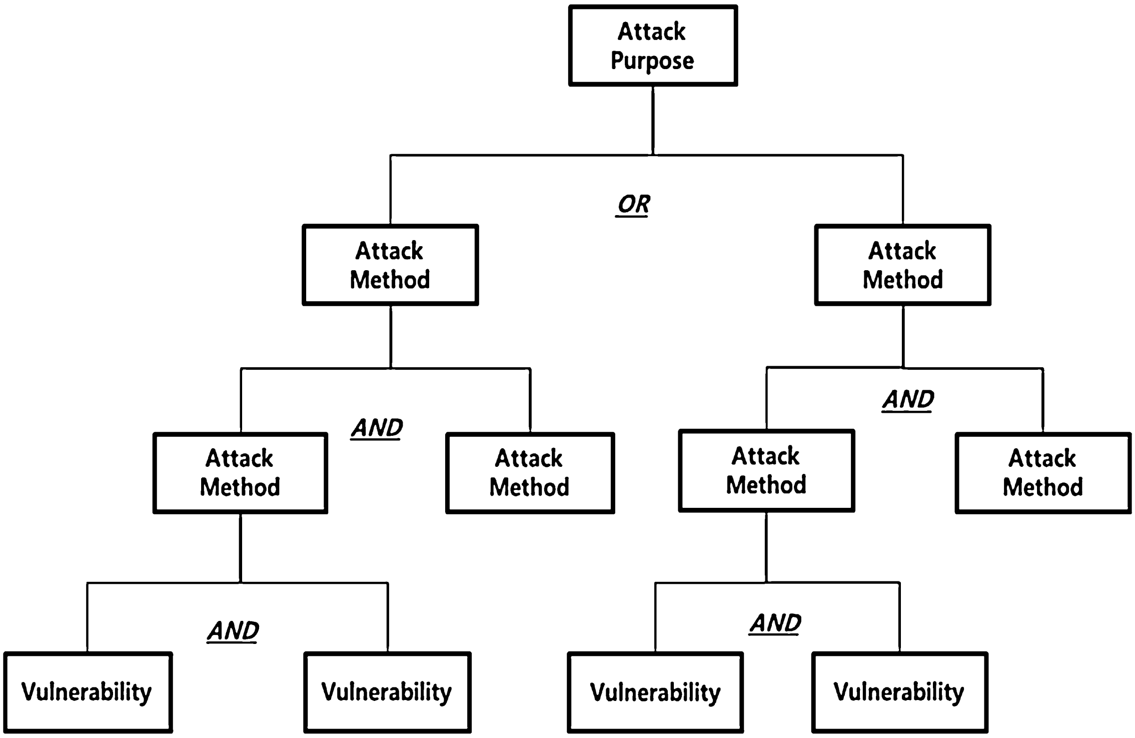

Fig. 3 Attack tree modeling for threat/vulnerabilities analysis of the smart car

3.1.3 Risk analysis

Categorization and mapping of threats to/vulnerabilities of each asset The vulnerabilities of an asset and the vulnerability paths of a threat are mapped based on the analysis to categorize the threats and vulnerabilities of each asset so as to define the relationship between the assets, threats and vulnerabilities, because the risk can be deduced through such relationships. GMITS (ISO13335) defines the relationship between the threats and vulnerabilities based on the assets. As such, this study also categories and maps the threats and vulnerabilities based on the assets of smart cars.

Calculation of risk level This study assess the risk using the risk calculation formula of GMITS (ISO13335) R = A×T×V (ISO/IEC 1998). The risk rating is calculated by multiplying the measured value by the threat/vulnerability evaluation. The range is 0.0–3.0.

3.1.4 Risk assessment

Security risk assessment calculation The risk rating was scaled to 0.0–3.0. A risk of $0.0 < R \leq 1.0$ was categorized as a low risk 'L' rating, while a risk of $1.0 < R \leq 2.0$ was categorized as a medium risk 'M' rating and a risk of $2.0 < R \leq 3.0$ was rated as a high risk 'H' rating. In the case of asset evaluation, only the highest evaluation point was reflected in calculating the risk. This reflects the evaluation of safety, privacy and operational to evaluate the asset's importance.

3.2 Comparison of two frameworks for analyzing automobile security risks

Wolf and Scheibel (2012) proposed a framework for analyzing the security risks of IT systems in an automobile. Table 4 shows a comparison of their framework and the framework proposed by this study.

Assessment method The framework proposed by Wolf and Scheibel (2012) qualitatively assesses the security risk. The framework proposed by this study includes the qualitative evaluation of assets and the calculation of the probability of threats and vulnerabilities. Since the threats and vulnerabilities are calculated in terms of probability using the attack tree, a more objective assessment is made possible.

Assessment procedure The framework proposed by Wolf and Scheibel (2012) assesses the risks based on the score of each element of AP (Attack Potential) and DP (Damage Potential) without the identification and categorization of threats and vulnerabilities, making it difficult to clearly distinguish the assets, threats and vulnerabilities. This study identifies and categories the assets, threats and vulnerabilities, and then assesses the security risk, which makes it easier to define each term and to distinguish the assets, threats and vulnerabilities.

Analysis method The framework proposed by Wolf and Scheibel (2012) referred to the CEM evaluation method for AP(Attack Potential) and used the SIL evaluation for DP (Damage Potential) to assess the risk. This study used the severity assessment technique of the EVITA project to evaluate the assets and attack tree analysis to evaluate the threats and vulnerabilities. Attack tree analysis enables the visual configuration and logical modeling of a hacking attack against a smart car.

Definition of risk The framework of Wolf and Scheibel (2012) defined a risk as R = (probability of an incident) × (expected losses caused by that incident). This study defined it as R = Asset (A) × Threat (T) × Vulnerability (V). The analysis method and type differ according to how a risk is defined.

4 An illustrative example: powertrain and infotainment

This study aggregated and analyzed the security threats and vulnerabilities deduced by the EVITA project and preceding studies, and conducted a quantitative analysis using an attack tree technique based on the reports of existing studies. The framework was applied only to vehicle velocity increase and personal information leakage, which are the leading threats. Table 5 summarizes the assets, threats and vulnerabilities of the cases used in this study.

As the study by literature reported that security threats and vulnerabilities exist without disclosing the attack

Table 4 Comparison of two frameworks

Type	Framework by Wolf and Scheibel (2012)	Framework proposed in this study
Assessment method	Qualitative	Combination of qualitative and quantitative assessment
Assessment procedure	Risk assessment through AP (Attack Potential) and DP (Damage Potential) analysis	Risk assessment using asset, threat, and vulnerability analysis
Analysis method	SIL (Safety Integrity Levels) and CEM (Common Evaluation Methodology)	Asset evaluation of EVITA and attack tree analysis
Definition of risk	Attack Potential (AP) × Damage Potential (DP)	Asset (A) × Threat (T) × Vulnerability (V)

scenarios of all threats and vulnerabilities, this study also applied only the threats of vehicle velocity increase and personal information leakage, which are the leading threats facing smart cars, based on the attack scenario used in their study. The threat of vehicle velocity increase affects the power train system, while the threat of personal information leakage affects the infotainment system. The threat of vehicle velocity increase affects the powertrain system through the three vulnerabilities of engine control (EC) firmware update vulnerability, Bluetooth vulnerability, and CAN network vulnerability; whereas the threat of personal information leakage affects the infotainment system through Bluetooth vulnerability by mobile connection and Bluetooth vulnerability by automatic USB execution.

4.1 Asset analysis

4.1.1 Asset identification and categorization

Table 6 shows the identification and categorization of the assets of smart cars. The assets were identified based on the ECU categorization table summarized (Johansson et al. 2005). The assets were the system installed inside the automobiles. Many ECUs were categorized into four types. A powertrain is the key asset which is responsible for the drive of the automobile. A chassis is a braking system and includes the brakes and steering system. A body can be divided into a convenience system and a safety system. In this study, the safety systems were grouped as parts of the body. The body itself includes the TPMS, sunroof and other systems. A smart car has an in-vehicle infotainment system which provides information and entertainment through various multimedia services and connection to mobile and IT devices. It is recognized as a system which transforms an automobile from a simple means of transport into a next-generation platform that provides various services similar to mobile devices (Kim and Han 2012).

4.1.2 Evaluation of importance of assets

Table 7 summarizes the asset importance evaluation items. This study referred to the evaluation of the EVITA project to evaluate of importance of the assets (EVITA 2009).

4.2 Threat/vulnerability analysis

4.2.1 Threat identification

Table 8 summarizes the security threats to smart cars and shows which actions the hackers take to accomplish their goals (Brooks et al. 2009). To identify and categorize

Table 5 Assets, threats and vulnerabilities of cases in this study

Asset	Threat	Vulnerability	Researcher
Powertrain	Vehicle velocity increase	Firmware update Bluetooth CAN network	Cho et al. (2012) Koscher et al. (2010) Miller and Valasek (2013)
Infotainment	Personal information leakage	Bluetooth (mobile connection) Bluetooth (automatic USB execution)	Studnia et al. (2013) Brooks et al. (2009) Checkoway et al. (2011) Cho et al. (2012) Koscher et al. (2010) Miller and Valasek (2013)

Table 6 Identification and Categorization of the Assets of Smart Cars

Asset	Description
Powertrain	A subsystem related to the drive of a vehicle. It includes the engine and transmission An ECU that controls the parts of a car, including the engine ECU, motor ECU and transmission ECU
Chassis	It consists of the parts responsible for the braking of a vehicle It includes ABS, ESC and EPS
Body	It is divided into the convenience system group and the manual safety system group The convenience system group is used by the driver or passenger for greater convenience during operation, while the manual safety system group increases the safety of the driver and passengers at the time of an accident
Infotainment	Multimedia system software such as navigation, DMB, iPod, and Bluetooth, which are installed in a vehicle to provide information and entertainment

security threats, it is necessary to analyze who attacks and for what reasons. As such, this study identified the purposes of attacks by analyzing who the attacker is and what the attacker does. The eventual goal that the attacker intends to accomplish through an attack then became the security threat faced by a smart car.

4.2.2 *Vulnerability identification*

This study identified the vulnerabilities on the basis of the studies conducted by Brooks et al. (2009), Checkoway et al. (2011), and Studnia et al. (2013). The vulnerability was defined based on which path an attacker takes and which system attributes or functions the attacker uses to intrude into the internal system of an automobile. Table 9 summarizes the vulnerabilities of a smart car, which are mostly related with vehicle velocity increase and personal information leakage.

4.2.3 *Attack tree modeling*

Modeling of vehicle velocity increase threat Fig. 4 shows the execution of an attack on vehicle velocity increase using vulnerability.

Attack tree modeling was performed after the threats and vulnerabilities had been identified and categorized. This study applied the case of a vehicle velocity increase, which is a major threat. The vehicle velocity increase was modeled using the attack scenario used in preceding studies (EVITA 2009; Cho et al. 2012; Koscher et al. 2010; Miller and Valasek 2013). The vulnerabilities arising from the threat of increased vehicle velocity include firmware updates, use of the CAN network, and use of Bluetooth.

Table 7 Asset importance evaluation items

Class	Safety	Privacy	Operational
1	No damage	Unauthorized access without data	No problem with operating the vehicle
2	Light injury	Unauthorized access to only anonymous data	A problem that can be recognized and identified by the driver (No problem with operating the vehicle)
3	Serious injury or life-threatening injury	Unauthorized access to data that can identify or track the vehicle or driver	Significant impact on vehicle performance (Great impact on vehicle operation)

Table 8 Threats to smart cars

Attacker	Action	Attack purpose
Thief	Car theft by hacking the antitheft system	Attack on a PKES system
Terrorist	Killing of VIPs by taking over the internal system or remote control through a zombie vehicle	Vehicle velocity increase Engine stop Manipulation of brakes
Greedy driver	Attaining the personal information of another vehicle or obstructing the traffic flow	TPMS attack Seizure of personal information Manipulation of brakes Engine stop
Vehicle manufacturer	Intentional accident involving the vehicle from a competitor or a leakage of ECU data	Vehicle velocity increase Engine stop Manipulation of brake

Table 9 Vulnerabilities of smart cars

Vulnerability	Description
Insufficient security of multimedia	Intrusion into an internal system using a USB or CD player containing a malware
Allowance of access privilege via an external network	Acquisition of the access privilege via an external network such as Bluetooth to intrude into an internal system or leak personal information from a car
Insufficient security of firmware update	Theft of data by manipulating the code or inserting a malware using ECU flashing, which can be a violation of the intellectual property of the ECU
Insufficient security of internal network	Security vulnerability due to a lack of encryption of the CAN network, which is an internal network of a vehicle

The three attack scenarios are configured of OR nodes concerning the threat of a vehicle velocity increase.

Figure 5 shows the execution of an attack on vehicle velocity increase using the firmware update vulnerability. When using the firmware update, the attack collects the code data of the EC (Engine Controller) first, and then inserts the malware to send the vehicle velocity increase message in the firmware. After that, when the driver updates the firmware with the OBD (on-board diagnostics) terminal in the wired or wireless connection, the EC generates an error and increases the vehicle's velocity. The OBD checks and controls the electrical/electronic operation status of the vehicle. Although initially it was used to maintain electronic parts such as the engine, it now plays the role of user interface for the trip computer, which informs the driver of various vehicle conditions.

Figure 6 shows the vehicle velocity increase using the Bluetooth vulnerability. To use Bluetooth, the infotainment system privilege is needed first. This can be obtained with the Bluetooth communication privilege or by connecting to Bluetooth through a mobile device to which a malicious SW has been downloaded. To obtain the Bluetooth communication privilege, Bluetooth is scanned, and the PIN number is obtained using the brute force attack. The attack can

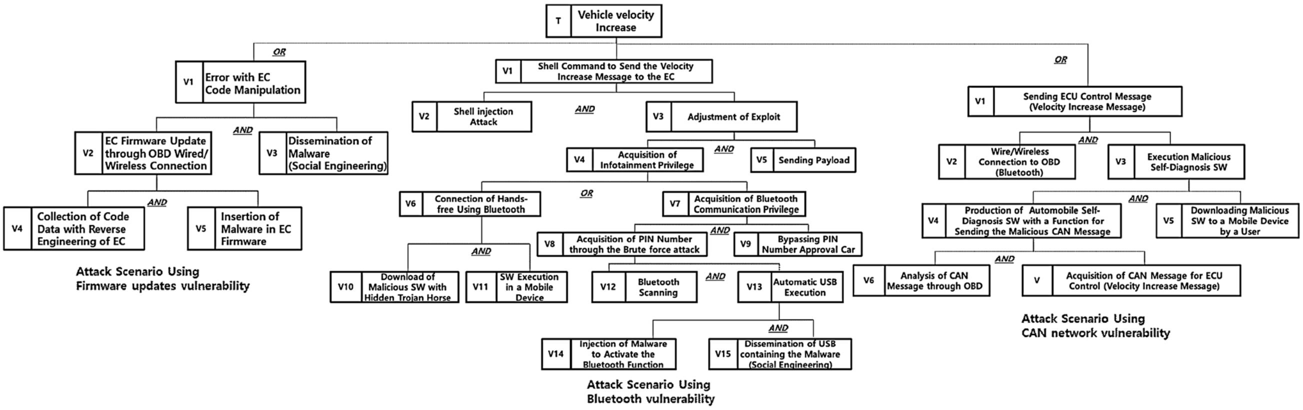
T Vehicle velocity Increase
OR
V1 Error with EC Code Manipulation
AND
V2 EC Firmware Update through OBD Wired/ Wireless Connection
V3 Dissemination of Malware (Social Engineering)
AND
V4 Collection of Code Data with Reverse Engineering of EC
V5 Insertion of Malware in EC Firmware
Attack Scenario Using Firmware updates vulnerability
V1 Shell Command to Send the Velocity Increase Message to the EC
AND
V2 Shell injection Attack
V3 Adjustment of Exploit
AND
V4 Acquisition of Infotainment Privilege
V5 Sending Payload
OR
V6 Connection of Hands-free Using Bluetooth
V7 Acquisition of Bluetooth Communication Privilege
AND
V10 Download of Malicious SW with Hidden Trojan Horse
V11 SW Execution in a Mobile Device
AND
V8 Acquisition of PIN Number through the Brute force attack
V9 Bypassing PIN Number Approval Car
AND
V12 Bluetooth Scanning
V13 Automatic USB Execution
AND
V14 Injection of Malware to Activate the Bluetooth Function
V15 Dissemination of USB containing the Malware (Social Engineering)
Attack Scenario Using Bluetooth vulnerability
OR
V1 Sending ECU Control Message (Velocity Increase Message)
AND
V2 Wire/Wireless Connection to OBD (Bluetooth)
V3 Execution Malicious Self-Diagnosis SW
AND
V4 Production of Automobile Self-Diagnosis SW with a Function for Sending the Malicious CAN Message
V5 Downloading Malicious SW to a Mobile Device by a User
AND
V6 Analysis of CAN Message through OBD
V Acquisition of CAN Message for ECU Control (Velocity Increase Message)
Attack Scenario Using CAN network vulnerability

Fig. 4 Vehicle velocity increase threat using vulnerability

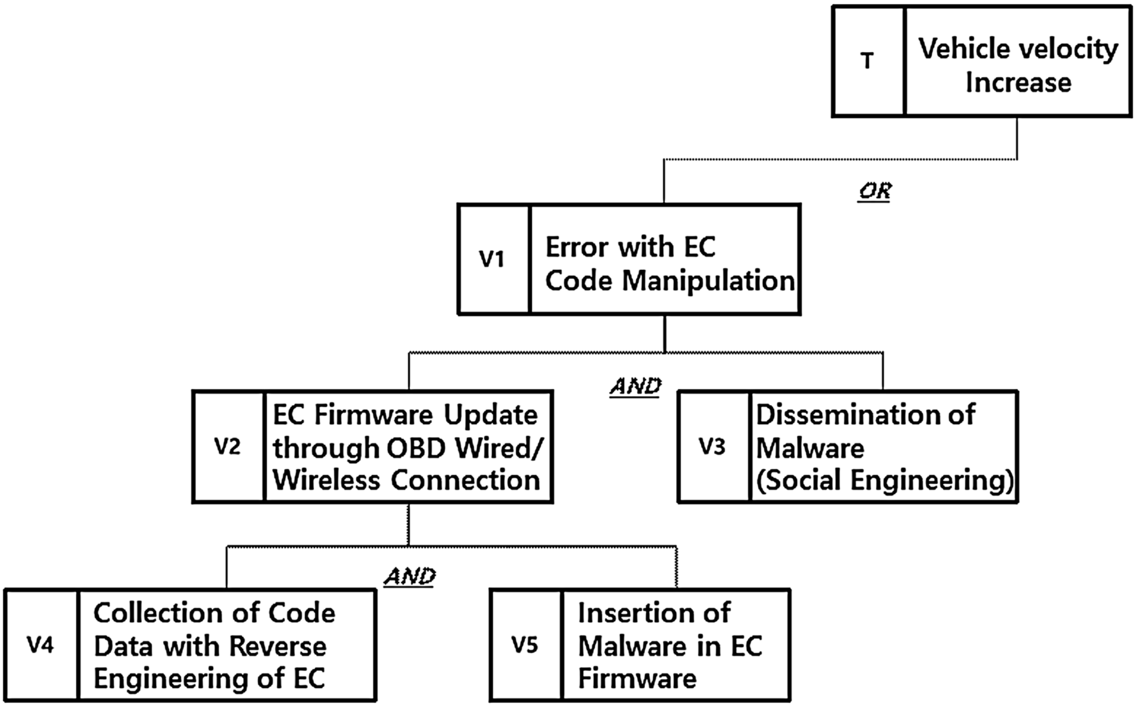
T Vehicle velocity Increase
OR
V1 Error with EC Code Manipulation
AND
V2 EC Firmware Update through OBD Wired/ Wireless Connection
V3 Dissemination of Malware (Social Engineering)
AND
V4 Collection of Code Data with Reverse Engineering of EC
V5 Insertion of Malware in EC Firmware

Fig. 5 Vehicle velocity increase threat using firmware updates vulnerability

intrude into the internal network of a vehicle by modifying the exploit code in the infotainment system. When the shell injection attack is modified, the message to increase the vehicle velocity is sent through the shell. Basically, the external network and internal network of a vehicle are separated. However, the external network can intrude upon the internal network because of the SAE J2534 standard (Miller and Valasek 2013). SAE J2534 provides the API and programming interface to enable communication with the network inside the automobiles. The US Environmental Protection Agency mandates adoption of the SAE J2534 standard for all new vehicles.

Figure 7 shows an vehicle velocity increase attack using the CAN network vulnerability. When a hacker uses the CAN network, the hacker first analyzes the CAN message, then uses the analyzed message to produce an automobile self-diagnosis SW with a malicious CAN message sending function. When a driver connects to a mobile device through a wired or wireless network after downloading the malicious SW, the hacker sends a message to increase the vehicle velocity through an automobile hacking program produced in advance.

Modeling of personal information leakage threat Personal information leakage was modeled using the attack scenarios of preceding studies (EVITA 2009; Cho et al. 2012; Koscher et al. 2010; Miller and Valasek 2013). The infotainment system is the head unit that manages the various information systems and contains CD player, USB, Bluetooth, etc. to provide the information and media system to the driver. The infotainment system can be connected to various external networks, thus enabling the leakage of personal information such as location data and private call recordings stored in the system. Figure 8 shows the result of the attack tree modeling of the personal information leakage threat, and indicates that attacks are possible using two types of vulnerabilities. In the case of the Bluetooth vulnerability via mobile connection, the attacker produces a malicious SW with a hidden Trojan horse, and uploads it to an application market from which the mobile application can be downloaded or sent to the driver. When the driver runs the malicious SW and connects the vehicle with a mobile phone through Bluetooth, the attacker can use the malicious SW to hack the vehicle's infotainment system and

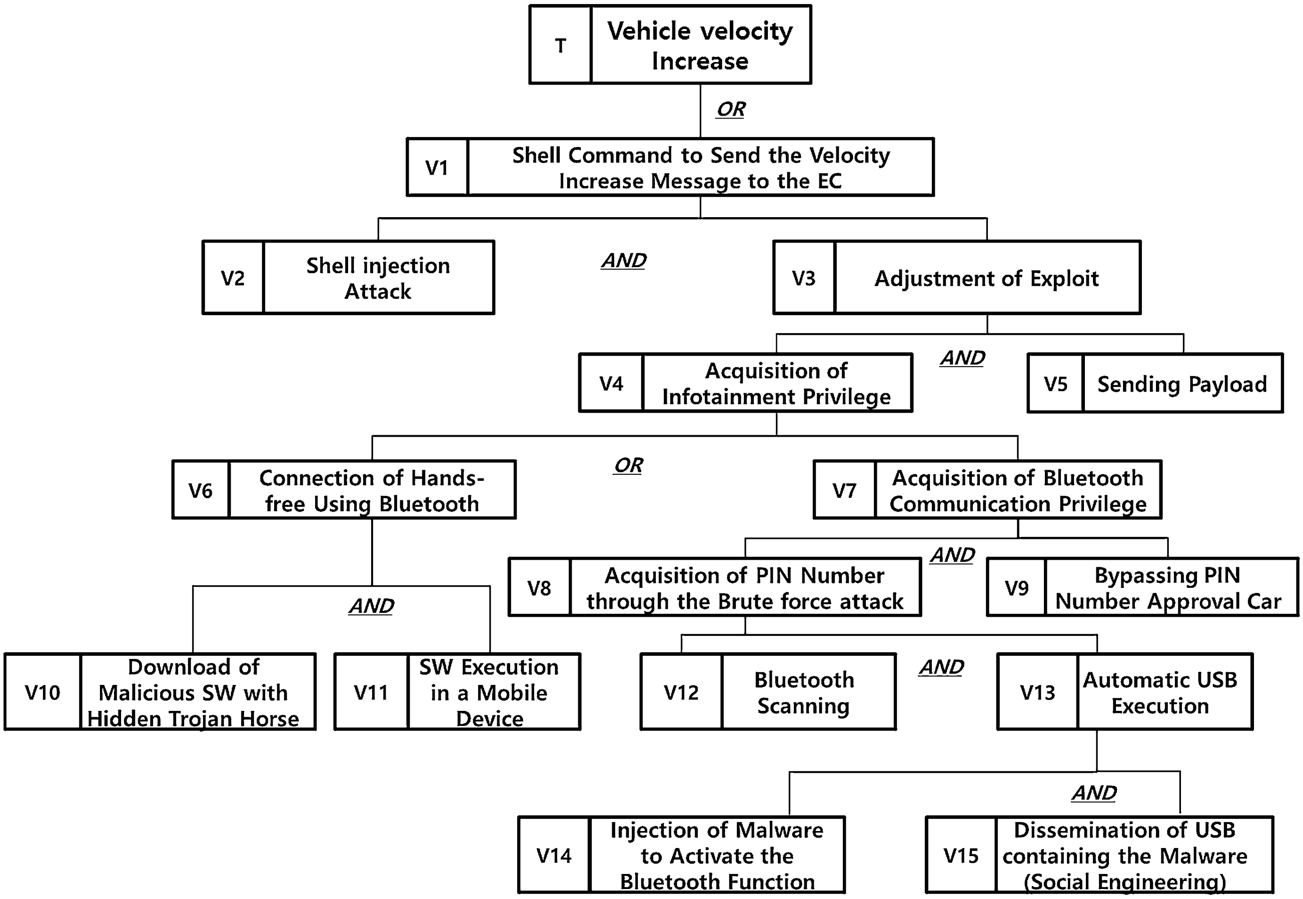
T
Vehicle velocity Increase
OR
V1
Shell Command to Send the Velocity Increase Message to the EC
V2
Shell injection Attack
AND
V3
Adjustment of Exploit
V4
Acquisition of Infotainment Privilege
AND
V5
Sending Payload
V6
Connection of Hands-free Using Bluetooth
OR
V7
Acquisition of Bluetooth Communication Privilege
AND
V8
Acquisition of PIN Number through the Brute force attack
V9
Bypassing PIN Number Approval Car
AND
V10
Download of Malicious SW with Hidden Trojan Horse
V11
SW Execution in a Mobile Device
V12
Bluetooth Scanning
AND
V13
Automatic USB Execution
AND
V14
Injection of Malware to Activate the Bluetooth Function
V15
Dissemination of USB containing the Malware (Social Engineering)

Fig. 6 Vehicle velocity increase using Bluetooth vulnerability

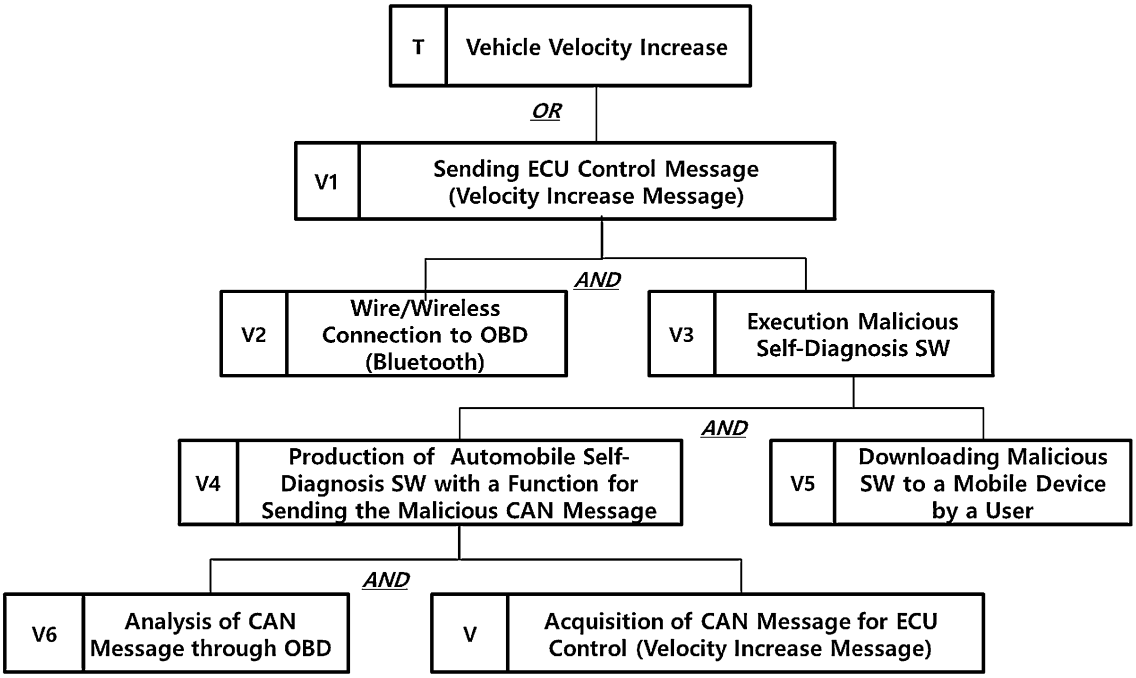
T
Vehicle Velocity Increase
OR
V1
Sending ECU Control Message (Velocity Increase Message)
AND
V2
Wire/Wireless Connection to OBD (Bluetooth)
V3
Execution Malicious Self-Diagnosis SW
AND
V4
Production of Automobile Self-Diagnosis SW with a Function for Sending the Malicious CAN Message
V5
Downloading Malicious SW to a Mobile Device by a User
AND
V6
Analysis of CAN Message through OBD
V
Acquisition of CAN Message for ECU Control (Velocity Increase Message)

Fig. 7 Vehicle velocity increase using CAN network vulnerability

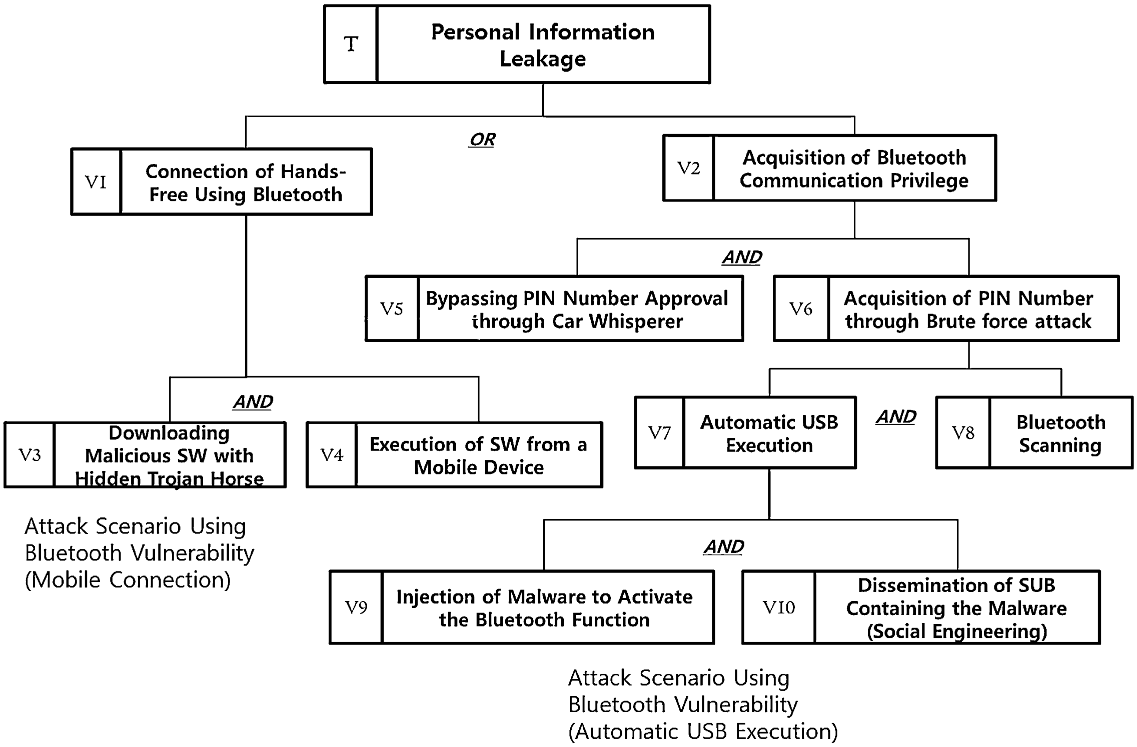
T
Personal Information Leakage
OR
VI
Connection of Hands-Free Using Bluetooth
V2
Acquisition of Bluetooth Communication Privilege
AND
V5
Bypassing PIN Number Approval through Car Whisperer
V6
Acquisition of PIN Number through Brute force attack
AND
V3
Downloading Malicious SW with Hidden Trojan Horse
V4
Execution of SW from a Mobile Device
AND
V7
Automatic USB Execution
V8
Bluetooth Scanning
AND
V9
Injection of Malware to Activate the Bluetooth Function
VI0
Dissemination of SUB Containing the Malware (Social Engineering)
Attack Scenario Using Bluetooth Vulnerability (Mobile Connection)
Attack Scenario Using Bluetooth Vulnerability (Automatic USB Execution)

Fig. 8 Personal information leakage using bluetooth vulnerability

access the driver's personal information including location data, vehicle ID, and the destination, starting point and stopover points stored in the navigation. In the case of the Bluetooth vulnerability through automatic USB execution, a malware designed to activate the Bluetooth function is injected into an MP3, and the USB containing the MP3 is delivered to a driver via a social engineering method. The driver runs the USB to listen to the MP3, which activates the Bluetooth function without the driver's knowledge. The attacker checks the Bluetooth in the vehicle through Bluetooth scanning and obtains the PIN number by brute force attack. Bluetooth demands the PIN number in the pairing process. In other words, the final connection is established after the driver's approval. However, the available car whisperer software can easily bypass this procedure. After obtaining the Bluetooth communication privilege, the attacker intrudes into the vehicle's infotainment system and leaks the personal information of the driver.

4.2.4 Threat evaluation

Evaluation of vehicle velocity increase threat After the attack tree modeling, the vehicle velocity increase threat is evaluated with three scenarios. Table 10 shows the result of the evaluation of the vehicle velocity increase threat after calculating the probability thereof using the attack tree model.

Evaluation of personal information leakage threat Table 11 shows the result of the evaluation of the personal information leakage threat by calculating the probability using the attack tree model.

4.2.5 Vulnerability evaluation

Evaluation of vulnerability of vehicle velocity increase threat The three vulnerabilities of the vehicle velocity increase threat were identified by identifying and categorizing the threats and vulnerabilities, and the threat was evaluated with attack tree modeling. The vulnerability was then evaluated by calculating the probability thereof using the attack tree. Table 12 shows the result of the evaluation of the vulnerabilities of vehicle velocity increase threat.

Evaluation of vulnerability of personal information leakage threat Table 13 shows the result of the evaluation of the vulnerabilities of the personal information leakage threat.

Table 10 Evaluation of vehicle velocity increase threat of smart cars

Vulnerability	Node	Calculation	Value
Firmware update	V2	1 − (1/2 + 1/2)	0
	V1	1 − ((1/2 × 1/2) + 1/2)	0.25
	T	1 − ((1/3 × 0.25) × 1/3 × 1/3)/(((1/3 × 0.25) × 1/3)+((1/3 × 0.25) × 1/3)+(1/3 × 1/3))	0.94
Bluetooth	V13	1 − (1/2 + 1/2)	0
	V8	1 − ((1/2 × 1/2) + 1/2)	0.25
	V7	1 − ((1/2 × 0.25) + 1/2)	0.375
	V4	1 − ((1/2 × 0.375) × (1/2 × 1/2))/((1/2 × 0.375)+(1/2 × 1/2))	0.893
	V3	1 − ((1/2 × 0.893) + 1/2)	0.053
	V1	1 − ((1/2 × 0.053) + 1/2)	0.47
	T	1 − ((1/3 × 0.47) × 1/3 × 10/3)/(((1/3 × 0.47) × 1/3)+((1/3 × 0.47) × 1/3)+(1/3 × 1/3))	0.91
CAN network	V4	1 − (1/2 + 1/2)	0
	V3	1 − ((1/2 × 1/2) + 1/2)	0.25
	V1	1 − ((1/2 × 0.25) + 1/2)	0.375
	T	1 − ((1/3 × 0.375) × 1/3 × 1/3)/(((1/3 × 0.375) × 1/3)+((1/3 × 0.375) × 1/3)+(1/3*1/3))	0.93

Table 11 Evaluation of personal information leakage threat of smart cars

Vulnerability	Node	Calculation	Value
Bluetooth vulnerability (mobile connection)	V1	1 − (1/2 + 1/2)	0
	T	1 − ((1/2 × 1/2) × 1/2)/((1/2 × 1/2) + 1/2)	0.83
Bluetooth vulnerability (automatic USB execution)	V7	1 − (1/2 + 1/2)	0
	V6	1 − ((1/2 × 1/2) + 1/2)	0.25
	V2	1 − ((1/2 × 0.25) + 1/2)	0.375
	T	1 − ((1/2 × 0.375) × 1/2)/((1/2 × 0.375) + 1/2)	0.86

4.3 Risk analysis

Risk analysis schematizes the risks and calculates the level of risk using the results of analyses of assets, threats and vulnerabilities.

4.3.1 Categorizing and mapping threat of each asset

The vulnerabilities of an asset and those of a threat are categorized and mapped. The threats of security risk of smart cars are shown in Fig. 9.

As regards the powertrain, the vehicle velocity threat and the engine stoppage threat exist. In the case of the chassis, the brake can be manipulated to stop the car. As for the body, the TPMS can be attacked to cause inconvenience to the driver during operation. In the case of infotainment, the personal information held in the system, such as the driver's favorite radio program, location data tracked through the navigation, or positions stored in the navigation, can be leaked.

4.3.2 Calculation of the risk level

The risk level R is calculated by evaluating the importance of assets and the threats and vulnerabilities identified by the analysis procedure. This study deduced the risk level of the vehicle velocity increase attack, which is a major threat for smart cars. The risk levels thus calculated are presented in Table 14.

4.4 Risk assessment

4.4.1 Security risk assessment calculation

The security risk rating of a smart car is presented in the security risk assessment framework as shown in Table 14. The risk level is scored in 0.0–3.0. A risk of $0.0 < R \leq 1.0$ was categorized as a low risk L rating, while a risk of $1.0 < R \leq 2.0$ was categorized as a medium risk M rating and a risk of $2.0 < R \leq 3.0$ was rated as a high risk H rating. The evaluation values of the assets, threats and vulnerabilities are multiplied and then graded into an L, M or H rating as the final assessment of the vehicle velocity increase threat and personal information leakage threat. This reflects the importance of the asset. In the case of an asset, the risk level is calculated by reflecting only the highest score. The reason for reflecting only the highest score is that the security threats should be considered from various angles in the case of an automobile; while security measures the part of the highest score should be focused on efficiency in consideration of which aspect is the most important for each asset when the security measures are established. For example, the safety (S) aspect received the highest score in the case of a powertrain, which shows that the focus should be on safety (S) rather than privacy (P) or operability (O) when it comes to establishing the security measures.

Table 13 Evaluation of vulnerability of personal information leakage threat

Vulnerability	Node	Calculation	Value
Bluetooth vulnerability (mobile connection)	V1	1/2 + 1/2	1
Bluetooth vulnerability (automatic USB execution)	V7	1/2 + 1/2	1
	V6	(1/2 × 1/2) + 1/2	0.75
	V2	((1/2 × 0.75) × 1/2) + 1/2	0.687

Powertrain system With regard to the powertrain asset, the presence of the vehicle velocity increase threat is caused by three vulnerabilities. In the evaluation of the asset's importance, safety (S) received 3 points, privacy (P) received 1 point, and operational (O) received 2 points (EVITA 2009). To evaluate the asset, only safety (S), which received the highest score, is reflected. This means that, since the powertrain is a key vehicle asset that greatly

Table 12 Evaluation of vulnerability of vehicle velocity increase threat

Vulnerability	Node	Calculation	Value
Firmware update	V2	1/2 + 1/2	1
	V1	(1/2 × 1/2) + 1/2	0.75
Bluetooth	V13	1/2 + 1/2	1
	V8	(1/2 × 1/2) + 1/2	0.75
	V7	((1/2 × 0.75) × 1/2) + 1/2	0.687
	V4	((1/2 × 0.687) × 1/2 × 1/2)/((1/2 × 0.687 × 1/2) + 1/2)	0.1278
	V3	((1/2 × 0.127) × 1/2 × 1/2 × 1/2) + 1/2	0.507
	V1	((1/2 × 0.507) × 1/2 × 1/2 × 1/2 × 1/2) + 1/2	0.515
CAN network	V4	1/2 + 1/2	1
	V3	(1/2 × 1/2) + 1/2	0.75
	V1	((1/2 × 0.75) × 1/2) + 1/2	0.687

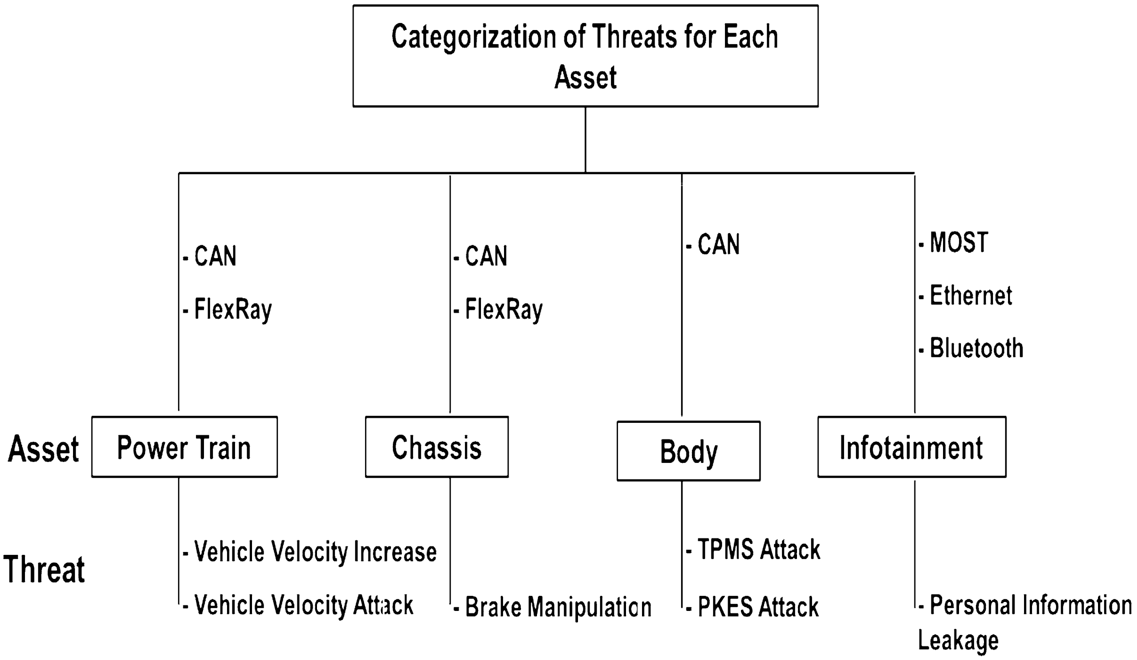

Fig. 9 Threat categorization and mapping for each asset

Table 14 Calculation of security risk assessment of smart cars

Type			Value				
Asset	Threat	Vulnerability	Asset (A)	Threat (T)	Vulnerability (V)	Risk (R)	Rating
Powertrain	Vehicle velocity increase	Firmware update	S = 3 P = 1 O = 2	0.94	0.75	2.11	**H**
		Bluetooth	S = 3 P = 1 O = 2	0.91	0.515	1.44	**M**
		CAN network	S = 3 P = 1 O = 2	0.93	0.687	1.94	**M**
Infotainment	Personal information leakage	Bluetooth (mobile connection)	S = 1 P = 3 O = 1	0.83	1	2.49	**H**
		Bluetooth (USB execution)	S = 1 P = 3 O = 1	0.86	0.687	1.77	**M**

affects the vehicle's safety rather than its privacy, the security measures should focus on safety.

In the evaluation of the vehicle velocity increase threat, the scores of the vulnerabilities were 0.94, 0.91 and 0.93 for the firmware update, Bluetooth, and CAN network, respectively. This indicates that the attack through the firmware update vulnerability was more threatening than attacks through other vulnerabilities. The threat evaluation tends to be high on average since the attack can be made using various vulnerabilities. The scores for the evaluation of the vulnerability to the vehicle velocity increase threat were 0.75, 0.515 and 0.687. The Bluetooth vulnerability scored low because there were many nodes by which the attack could reach its final goal. In the case of the firmware update, there were fewer nodes, meaning that the possibility of intrusion, i.e., the probability of success, was high, resulting in a high score in the vulnerability evaluation. The final risk levels were 2.11, 1.44 and 1.94 for the ratings of H, M and M, respectively. Thus, the security countermeasures for the vehicle velocity increase threat existing in the powertrain systems should focus on the safety aspect of the firmware update vulnerability.

Infotainment system In the infotainment system, the presence of the personal information leakage threat is caused by two vulnerabilities. In the evaluation of the asset's importance, safety (S) received 1 point, privacy (P) received 3 points, and operational (O) received 1 point (EVITA 2009). To evaluate the asset, only privacy (P), which received the highest score, is reflected, which means that security measures for the information system should focus on the privacy aspect since the information system contains the personal information of the driver.

In the evaluation of the personal information leakage threat, the scores of the vulnerabilities were 0.83 and 0.86 for the Bluetooth (mobile connection) and Bluetooth (USB execution), respectively, indicating that the Bluetooth vulnerability through automatic USB execution was more threatening. That is because the Bluetooth vulnerability through automatic USB execution becomes more threatening as it uses ever more diverse methods and vulnerabilities. The scores of the vulnerability evaluation of the personal information leakage threat were 1 and 0.687. The mobile connection showed a higher score since the infotainment system can be hacked immediately when the driver connects to Bluetooth.

The final risk levels were 2.49 and 1.77 for the ratings of H and M, respectively. The security countermeasures to the personal information leakage threat to the infotainment system should be established with a focus on the privacy aspect, and the vulnerability of Bluetooth through mobile connection should be rectified first.

5 Conclusion

5.1 Conclusion and implications

As ever more ICTs are being applied to automobiles, automobiles are gradually being transformed into smart cars, with the result that viruses or hacking techniques that were previously only used to attack existing ICTs are now being used to attack automobiles as well. The possibility of automobile hacking and the existence of various threats have been disclosed through penetration testing in preceding studies by experts. As the possibility of hacking smart cars is increasing, security technologies to cope with them are also being developed. However, it is unrealistic in terms of both cost and efficiency to apply every available security measure to all smart cars. To establish effective security measures, risk management-based measures are needed, with the adoption of a security risk assessment that measures and analyzes the level of risk being more important than anything else. As such, this paper proposes a security risk assessment framework for smart cars to facilitate the efficient formulation of security measures. The significance of this study lies in the fact that it proposes a method of logically modeling hacking attacks against automobiles and of evaluating security threats and vulnerabilities, by using the attack tree analysis technique. It then presents the framework for measuring and assessing the security risks to automobiles for use as a reference when establishing efficient security measures. Finally, the framework was applied in cases to categorize the security threats and vulnerabilities for each asset, and then to assess the risk.

5.2 Limitations of the study and future research

This study has limitations in that it was conducted on the assumption that various factors—such as the technical capability of the attacker and costs—were the same. Therefore, different factors were not included in the scope of the research, and only attack scenario-based studies were carried out. Second, it studied the basic security threats and vulnerabilities of automobiles without taking into account the fact that the characteristics and functions of automobiles may differ depending on the manufacturer. Although automobile systems do not greatly differ in the case of automobile production, each automobile manufacturer nevertheless uses a slightly different system. Based on the automobile hacking scenarios used in earlier studies, this study limited the scope of its research to smart cars equipped with the basic functions. To overcome such limitations, any future researches will need to study the risk assessment framework in greater depth by adding the technical capability of the attacker and the cost, and/or by reflecting the specific characteristics of each manufacturer therein.

References

Bernardo DV, Hoang DB (2012) Multi-layer security analysis and experimentation of high speed protocol data transfer for GRID. Int J Grid Util Comput 3(2–3):81–88

Bharadiya B, Maity N, Hansdahs RC (2014) An authentication protocol for vehicular ad hoc networks with heterogeneous anonymity requirements. Int J Space-Based Situat Comput 4(1):1–14

Brooks RR, Sander S, Deng J, Taiber J (2009) Automobile security concerns. IEEE Veh Technol Mag 4(2):52–64

Cha BR, Kim JW (2013) Handling and analysis of fake multimedia contents threats with collective intelligence in P2P file sharing environments. Int J Grid Util Comput 4(1):1–9

Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S, Kohno T (2011) Comprehensive experimental analyses of automotive attack surfaces. In: Proceedings of the USENIX security symposium; 8–12 August, San Francisco, pp 77–92

Chen YJ, Liao GY, Cheng TC (2009) Risk assessment on instrumentation and control network security management system for nuclear power plants. In: 2009 43rd Annual IEEE/IFIP International Carnahan conference on security technology; 5–8 October, 2009. IEEE, Zurich, pp 261–264

Cho AR, Cho HJ, Son YD, Lee DH (2012) A message authentication and key distribution mechanism secure against CAN bus attack. J Korea Inst Info Sec Cryptol 22(5):1057–1068 (in **Korean**)

EVITA (2009) Security Requirements for Automotive on-board Networks based on Dark-side Scenarios EVITA Deliverable D2. 3. EVIPA Project

Francillon A, Danev B, Capkun S (2011) Relay attacks on passive keyless entry and start systems in modern cars. In: Network and distributed system security symposium

Hahn A, Govindarasu M (2011) Cyber attack exposure evaluation framework for the smart grid. IEEE Trans Smart Grid 2(4):835–843

Han H (2012) SmartCar. KISTI Mark Rep 2(4):3–7 (in **Korean**)

Hossain I, Mahmud SM (2007) Analysis of a secure software upload technique in advanced vehicles using wireless links. In: IEEE intelligent transportation systems conference; 30 September–3 October. IEEE, Seattle, WA, pp 1010–1015

Johansson KH, Törngren M, Nielsen L (2005) Vehicle applications of controller area network: handbook of networked and embedded control systems. Birkhäuser, Boston, pp 741–765

Kang YD, Jeong KD (2010) Development of cyber security assessment methodology for the instrumentation & control systems in nuclear power plants. J Acad Ind Technol 11(9):3451–3457

Kang DJ, Lee JJ, Lee Y, Lee IS, Kim HK (2013) Quantitative methodology to assess cyber security risks of SCADA system in electric power industry. Journal of the Korea Institute of Information Cryptology 23(3):445–457 (in **Korean**)

KDB Research (2014) Smart car world market 230 trillion Korean won annual growth of 6.7%, http://www.yonhapnews.co.kr/economy/2014/05/04/0301000000AKR20140504025000002.HTML. Accessed 7 May 2014

Ketel M (2008) IT security risk management. In: Proceedings of the 46th Annual Southeast Regional Conference; 28 March. ACM, New York, pp 373–376

Kim JW, Han TM (2012) Trends of the standard open platform for in-vehicle infotainment and GENIVI based human machine interface. J KIISE Softw Appl 39(6):444–452 (in **Korean**)

Kim GJ, Lee DS (2014) Car security technology research trends by reviewing international conferences such as escar. Rev Korea Ins Info Sec Cryptol 24(2):7–20 (in **Korean**)

Kim ST, Jun MS, Park DW (2008) A study on the security assessment for information system risk management and budget management. J Korea Soc Comput Info 16(1):69–77

Kim KA, Lee DS, Nam KK (2011) ICS security risk analysis using attack tree. J Info Sec 11(6):53–58 (in **Korean**)

Kim JE, Chun BJ, Park SB (2013) Secure diagnostic implementation for automotive ECU with crypto library. Korea Society Automotive Engineers2013 Annual Conference; 20–22 November, Ilsan, South Korea: 1136–1144 (in **Korean**)

Ko JB, Lee SK, Shon TS (2013) Security threat evaluation for smartgrid control system. J Korea Ins Info Cryptol 23(5):873–883 (in **Korean**)

Koscher K, Czeskis A, Roesner F, Patel S, Kohno T (2010) Experimental security analysis of a modern automobile. In: 2010 IEEE Symposium on Security and Privacy; 16–19 May. IEEE, Oakland, pp 447–462

Li W, Huang J, You W (2010) Attack modeling for electric power information networks. In: 2010 International Conference on Power System Technology; 24–28 October, IEEE, Hangzhou, pp 1–5

Lim WW, Kim JS, Kim SJ, Oh HK (2011) Reduced RSU-dependency authentication protocol to enhance vehicle privacy in VANET. J Korea Ins Info Cryptol 21(6):21–34 (in **Korean**)

Lv WP, Li WM (2011) Space based information system security risk evaluation based on improved attack trees. In: 2011 Third International Conference on Multimedia Information Networking and Security; 4–6 November. IEEE, Shanghai, pp 480–483

Miller C, Valasek C (2013) Adventures in automotive networks and control units. . http://illmatics.com/car_hacking.pdf. Accessed on 13 Dec 2016

Narita M, Bista BB, Takata T (2013) A practical study on noise-tolerant PN code-based localisation attacks to internet threat monitors. Int J Space-Based Situat Comput 3(4):215–226.

Nilsson DK, Larson UE (2008) Secure firmware updates over the air in intelligent vehicles. In: IEEE International Conference on Communication; 19–23 May. IEEE, Beijing, pp 380–384

NIST (2002), Risk management guide for information technology system, NIST SP800-30

Patsakis C, Dellios K, Bouroche M (2014) Towards a distributed secure in-vehicle communication architecture for modern vehicles. Comput Secur 40:60–74

Petrlic R, Sekula S, Sorge C (2013) A privacy-friendly architecture for future cloud computing. Int J Grid Util Comput 4(4):265–277

Pudar S, Manimaran G, Liu CC (2009) PENET: a practical method and tool for integrated modeling of security attacks and countermeasures. Comput Secur 28(8):754–771

Ray PD, Harnoor R, Hentea M (2010) Smart power grid security: a unified risk management approach. In: 2010 International Carnahan Conference on Security Technology; 18–21 October. IEEE, Barcelona, pp 276–285

Raya M, Hubaux JP (2007) Securing vehicular ad hoc networks. J Comput Secur 15(1):39–68

Ren D, Du SU, Zhu H (2011) A novel attack tree based risk assessment approach for location privacy preservation in the VANETs. In: 2011 International Conference on Communications; 5–9 June, Kyoto. IEEE, Japan, pp 1–5

Rouf I, Miller R, Mustafaa H, Taylor T, Oh S, Xu W, Gruteser M, Trappe W, Seskar I (2010) Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. 19th USENIX Security Symposium; 11–13 August, Washington, pp 323–338

Roy A, Kim DS, Trivedi KS (2010) ACT: Attack countermeasure trees for information assurance analysis. In: IEEE Conference on Computer Communications Workshops; 15–19 March. IEEE, San Diego, pp 1–2

Schneier B (1999) Attack trees. Dr Dobb's Journal 24(12):21–29

Studnia I, Nicomette V, Alata E, Deswarte Y, Kaâniche M, Laarouchi Y (2013) Survey on security threats and protection mechanisms in embedded automotive networks. In: 2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop; 24–27 June. IEEE, Budapest, pp 1–12

Ten CW, Liu CC, Govindarasu M (2007) Vulnerability assessment of cyber security for SCADA systems using attack trees. In: IEEE Conference on Power Engineering Society General Meeting; 24–28 June, Tampa, FL. IEEE, USA, pp 1–8

Uhm JH (2012) An architecture of a dynamic cyber attack tree: Attributes approach. J Korea Inst Info Cryptol 21(3):67–74 (in **Korean**).

Viduto V, Maple C, Huang W (2011) Managing threats by the use of visualisation techniques. Int J Space-Based Situ Comput 1(2–3):204–212

Weiss JD (1991) A system security engineering process. In: Proceedings of the 14th National Computer Security Conference; 1–4 October, Washington, D.C., pp 572–581

Wi MS, Kim DS, Park JS (2013) Security analysis of AMI using ACT. J Korea Inst Info Cryptol 23(4):639–653 (in **Korean**)

Wolf M, Gendrullis T (2011) Design, implementation, and evaluation of a vehicular hardware security module. In: International Conference on Information Security and Cryptology; 30 November–2 December, Seoul, South Korea, pp 302–318

Wolf M, Scheibel M (2012) A systematic approach to a quantified security risk analysis for vehicular IT systems. In: Automotive-Safety and Security; 14–15 November, Karlsruhe, pp 195–210