Measures for Automaker's Legal Risks from Security Threats in Connected Car Development Lifecycle

Dong Hee Kim[1], Seung Jo Baek[2], and Jongin Lim[3]
[1]National Security Research Institute
P.O.Box 1, Yuseong, Daejeon, 34188 - Korea
[e-mail: dh_kim@nsr.re.kr]
[2, 3]Graduate School of Information Security, Korea University
Anam-ro 145, Sungbuk-gu, 02841 - Korea
[e-mail: nomadvirus@korea.ac.kr, jilim@korea.ac.kr]
*Corresponding author: Jongin Lim

Received June 30, 2016; revised October 19, 2016; accepted December 8, 2016; published February 28, 2017

Abstract

To improve passenger convenience and safety, today's vehicle is evolving into a "connected vehicle," which mounts various sensors, electronic control devices, and wired/wireless communication devices. However, as the number of connections to external networks via the various electronic devices of connected vehicles increases and the internal structures of vehicles become more complex, there is an increasing chance of encountering issues such as malfunctions due to various functional defects and hacking. Recalls and indemnifications due to such hacking or defects, which may occur as vehicles evolve into connected vehicles, are becoming a new risk for automakers, causing devastating financial losses. Therefore, automakers need to make voluntary efforts to comply with security ethics and strengthen their responsibilities. In this study, we investigated potential security issues that may occur under a connected vehicle environment (vehicle-to-vehicle, vehicle-to-infrastructure, and internal communication). Furthermore, we analyzed several case studies related to automaker's legal risks and responsibilities and identified the security requirements and necessary roles to be played by each player in the automobile development process (design, manufacturing, sales, and post-sales management) to enhance their responsibility, along with measures to manage their legal risks.

Keywords: Connected Vehicle Security, Legal Risks, Liability, Responsibility

https://doi.org/10.3837/tiis.2017.02.013 **ISSN : 1976-7277**

1. Introduction

Passenger vehicles represent one of the most important methods of transportation today and are considered to be additional "living spaces" in daily life. To improve passenger convenience and safety, such vehicles are constantly evolving through the convergence of various advanced technologies. A variety of sensors such as tire pressure management sensors (TPMSs) and lane departure warning systems (LDWSs), along with electronic control units (ECUs), wired/wireless network interfaces, and infotainment systems, to improve safety and convenience are making vehicles more "connected" and "smarter." The trend of convergence between vehicles and information and communications technology (ICT) has created various new terms, including "smart cars," "connected vehicles," and "self-driving cars."[1]

The paradigm-shift to connected vehicles has also changed the possibility and level of security risks in the automotive environment. Auto manufacturers have started to create a new ecosystem involving collaborations between information technology (IT) companies, network operators, etc., along with convergence between the automotive industry and others. In addition, various sensors, ECUs, and IT services are being linked together. This increases the connections with the Internet and other unsecure networks, as well as the complexity of the internal structure in connected vehicles [1]. These are very sensitive issues, which are gaining more attention. Practically, studies related to vehicle security and hacking have been introduced in numerous security conferences, including BlackHat and Defcon. In addition, some drivers who experienced malfunctions and system stoppages caused by security flaws in the ECUs or CANBUS of vehicles have submitted class actions against manufacturers to force recalls. The US Congress is in the process of passing legislation to enforce "The Security and Privacy in Your Car (SPY Car) Act" after the occurrence of the Fiat-Chrysler hacking issue [2]. Vehicle security issues can become a significant management risk for manufacturers. Therefore, there should be efforts to strengthen their responsibilities in relation to potential threats.

This article will discuss the legal issues that may arise from security threats under a connected vehicle environment and propose measures to reinforce corporate responsibilities to reduce such risks. This article is organized as follows. Section 2 considers vehicle security threats and the relevant corporate responsibilities. In section 3, we propose measures to strengthen corporate responsibilities to reduce such risks. Section 4 presents some conclusions.

2. Security Threats in Connected Vehicle

As mentioned in section 1, there have been many studies on vehicle security issues such as unauthorized access by sniffing during communication between external or internal sensors and ECUs, and vehicle stoppages or malfunctions because of infections with malicious code. Rouf (2010) analyzed packet spoofing, which involved tracing the driving path vulnerabilities

[1] Generally, connected vehicles are defined as "vehicles with network interfaces like Wi-Fi, LTE, Bluetooth, etc., to communicate with various devices, external infrastructures, or services such as the cloud to improve safety and convenience." Although the term "smart car" is often regarded as synonomous with "connected vehicle," the term "smart car" is actually more comprehensive because it includes connected vehicles as well as infotainment systems and self-driving cars. We limited the scope of this study to "connected vehicles" and excluded smart cars or self-driving cars.

by sniffing a vehicle's wireless communication between the TPMS and ECU [8]. Checkoway (2011) found the security threats in inner-network systems such as OBD-II port, CANBUS packet, CD players, and Bluetooth, along with telematics systems using mobile networks [9]. Tyagi (2014) analyzed a vehicle-to-vehicle (V2V) communication environment to make denial of service (DoS) attacks using jamming signals, as well as intercepting and forging message packets to monitor the driving path and infringe on privacy [10]. Petit (2015) identified the attack surface of the security threats in vehicles, and then analyzed their feasibility, ease of detection, and probability of success and rated each item [11]. Jaballah (2014) classified the possible attacks on in-vehicular communications, which included masquerading, DoS, sending false information to other vehicles, and tracking the location by disclosing the vehicle's ID [27]. Calandriello (2011) identified the vulnerabilities of vehicular communication systems in relation to jeopardizing users' privacy by injecting beacons with false information, tracking locations by collecting vehicle messages, etc. [28].

Table 1. Studies on security threats related to vehicles

Category	Security Threats	References
V2V/V2I	Interrupting communication (or computing) between vehicles by using jammers (e.g., DoS attacks)	[10][11][12][24][27]
	Causing accidents by forging or modifying communication messages between vehicles	[10][11][12][28]
	Violating driver's privacy by illegally monitoring driving information	[10][27][28]
	Bypassing authentication or unauthorized access to cellular network by misuse of communication protocol vulnerabilities in manufacturer's telematics call center (TCC)	[9]
	Physically extracting and re-using the certificate and key of the vehicle	[12]
	Forging and modifying messages by manipulating a vehicle's onboard software	[12]
Internal	Taking over the ECU authority while connecting to the OBD-II port	[9]
	Running executable code while playing CDs with malware infected WMA or MP3 files	[9]
	Causing malfunctions in telematics by injecting abnormal strcpy command while using Bluetooth control	[9]
	Infecting a vehicle's internal system while connecting to a smartphone application with malicious code	[9]
	Gaining remote access to the vehicle and controlling internal systems by intercepting a PIN while Bluetooth pairing	[9]
	Causing malfunctions by transferring a manipulated TPMS packet to the ECU through CANBUS	[9]
	Privacy infringement while connecting with social media and transferring driving information	[12]
	Privacy infringement by intercepting TPMS information while remotely transferring from RFID sensor to ECU	[24]

Studies with fresh views on these issues are being performed because automobile hacking is gaining attention from related organizations and security companies. In 2011, the U.S. Department of Transportation (DoT) analyzed the security threats that may arise from the intelligent transportation system (ITS) from a user and system point of view, and concluded that secure and reliable data transmission is a security requirement [12]. In addition, in 2014, the security company IOActive found security weaknesses in major automobile components such as the anti-theft device, remote key, TPMS, Bluetooth, audio system, and telematics, and released the test results for 20 major vehicles on the automobile market [13]. The automobile security threats discussed above can be classified based on the type of connected vehicle, as listed in **Table 1**.

3. Legal Risks in Connected Vehicle Security Issues

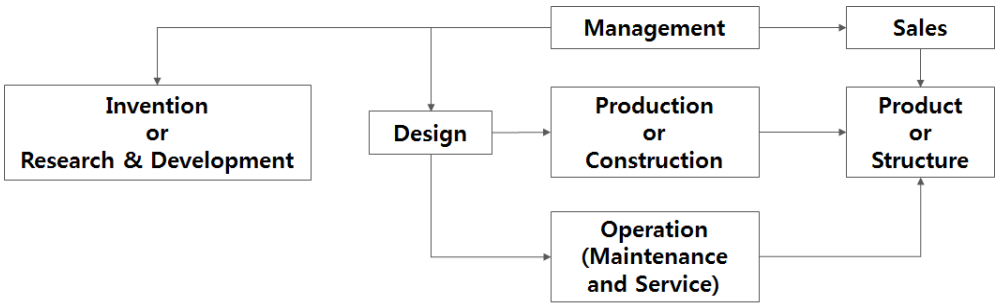
To maximize driver convenience and safety in the vehicles that are currently being released, automobile manufacturers load 70–100 ECUs in each vehicle in order to collect and process data from various sensors and communication devices in real time. This has resulted in increasing malfunctions due to unexpected errors or defects. In this section, we investigate the automobile manufacturing process, emerging security threats, lawsuits, and related cases that have arisen as a result of such security issues and defects and analyze the legal risks of the related business entities.

3.1 Automobile development process

Before examining the security issues and legal risks of automobiles, we need a good understanding of the automobile development process and the players at each stage. In this section, we describe the product (automobile) development process and the roles of the players at each stage. This is necessary to analyze the legal risks for a corporation that may result from security issues.

3.1.1 General product/system development process

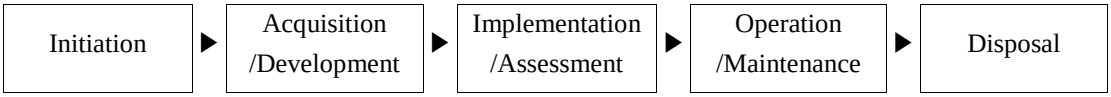
Because of the use of mass production and the growing demand for customized production, product development in traditional manufacturing has become a formal process, to which engineering techniques are applied. A representative example was given by Durbin (1991), who classified an engineering-based new product development process according to the roles and functions of the developer (engineer), as invention or research & development, design, production, sales, operation, and management, as shown below [3].



Phase	Purpose
Invention/R&D	Securing source technologies through innovative R&D or new invention before creating concepts or designing products
Design	Determining basic features and development direction of the new product
Production & Construction	Implementing and manufacturing products on the basis of the results obtained in the “Design” phase
Operation & Management	Testing, providing services and maintenance for, and selling the product ob tained in the “Production & Construction” phase

Fig. 1. Product development process

In addition, the National Institute of Standards and Technology (NIST) specifies the security requirements that need to be considered for system development, according to the system development life cycle (SDLC) from Special Publication (SP) 800-64, as shown below [4].



Phase	Purpose
Initiation	Clearly document the purpose and requirements of system development
Acquisition /Development	Design, purchase, and develop based on the purpose and requirements of the system
Implementation /Assessment	Install and deploy the system after testing
Operation /Maintenance	Operate the system in the field for the purpose of introduction
Disposal	Discard or replace the developed system after expiration

Fig. 2. System development life cycle (NIST)

3.1.2 Automobile development process

The process of automobile development is similar to that of general product development. In the auto industry, ISO/TS 16949 is used [5], which is legislation designed to enhance the quality during the auto manufacturing process based on the quality management system (ISO9001). In addition, the Automotive Industry Group (AIAG), which is led by global automakers such as Chrysler, Ford, GM, Toyota, Honda, and Nissan, has prepared an automobile development process guideline based on ISO/TS 16949, as shown below [6].

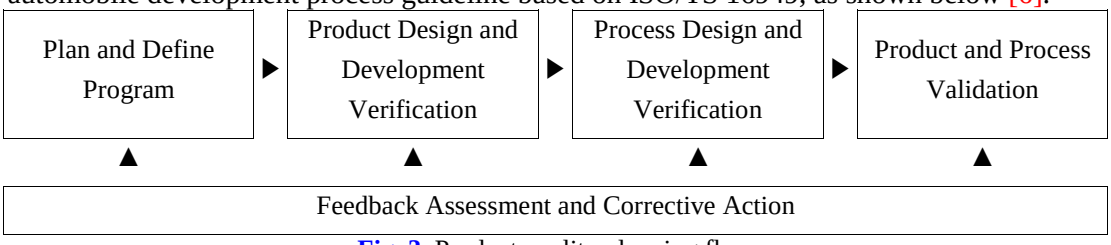


Fig. 3. Product quality planning flow

Furthermore, regarding functional safety, ISO26262, which is legislation to guarantee safety and prevent accidents that may rise from automobile software defects or malfunctions, suggests a process that tests the safety during automobile system and software development based on the V-model of IEC 61508 [7].

Based on various studies and the existing development processes for general products, systems, and automobiles, we can learn that there is a common process by which customers' requests for products and automobiles are incorporated into the design, and continuous maintenance or management is provided post-manufacturing and sales. Based on such an analysis, the automobile development process can be generalized, which allows the players at each stage to be categorized as auto makers (including OEMs), auto parts suppliers, and others (telecommunication company, application developer, traffic monitoring department or company), with the definitions and roles shown below.

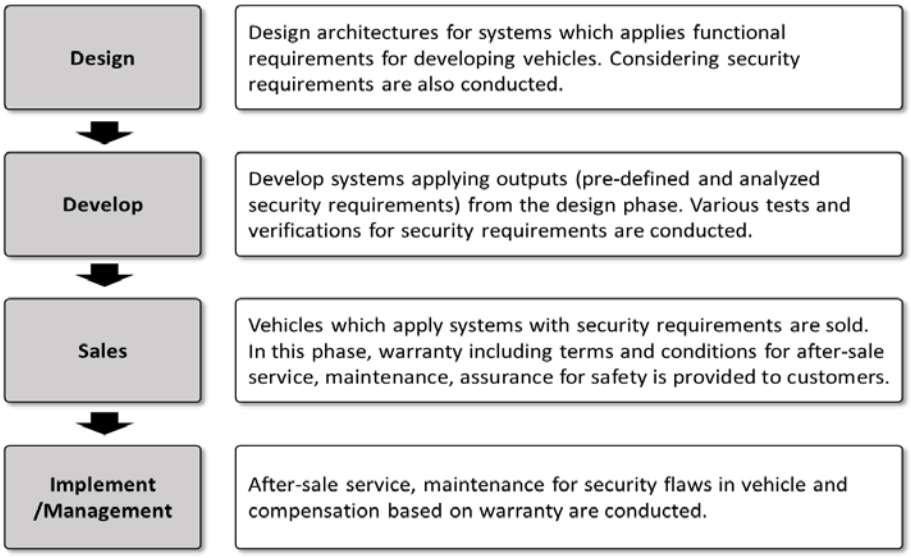


Fig. 4. Vehicle development life cycle

Table 2. Roles of OEMs, parts suppliers, and 3rd parties in life cycle

Phase/Players	OEM	Parts Supplier	3rd Party (App Dev, Telco, etc)
Design	Designing the overall vehicle (assembling the parts and systems)	Designing each part and system to meet OEM requirements	Designing applications and communication architectures to meet OEM requirements
Develop	Developing the overall length of the vehicle and suitable infrastructures for the designed architecture	Developing each parts and systems to meet OEM requirements	Developing applications and communication architectures to meet OEM requirements

Sales	Establishing sales and maintenance warranties for consumers	Supplying parts and systems for complete vehicles by contracting with OEMs	Supplying applications and communication infrastructures for complete vehicles by contracting with OEMs
Implement /Management	Implementing warranties of overall defects, damages, and replacement parts for the vehicle	Supplying and supplementing parts, re-designing systems of the vehicle by contracting with OEMs	Application updates and management, improving communication model and quality by the SLA with OEMs

3.2 Responsibility issues and relevant cases regarding automobile security

There is a growing concern that the previously mentioned automobile security threats may not simply remain the outcome of theoretical research but might be realized in our daily lives. Automobile security issues can cause malfunctions in vehicles, which may directly lead to casualties or economic loss. Thus, it is crucial to determine whether such security issues involve liability issues, and if so, which player within the automobile development process is responsible for them.

The liability of an automobile security issue can be determined by considering the contract between the automaker or vendor and the purchaser; whether there was any infringement; whether the automaker, vendor, and purchaser were legitimate; and whether there was at least a minimal effort to resolve the issue.

The key responsible players regarding automobile security issues can be categorized as the user, supplier, and third party. First, a user may arbitrarily manipulate or modify major electronic control devices such as the ECU, different kinds of sensors, or those related to infotainment, thereby causing the default security setup originally provided at the initial vehicle release to inactivate or become vulnerable to being bypassed. We will not deal with security issues resulting from the carelessness or intended manipulation of users because the user will be fully responsible in such cases. Second, suppliers, including automakers that design, develop, and sell automobiles, as well as auto parts developers and suppliers, may not take any security features into account when they manufacture vehicles, hardware, and software products, leading to unexpected security defects. Finally, third parties such as hackers or an insider with malicious intent may intentionally access and manipulate the vehicle system without authorization to cause a malfunction. In these cases, the third party will be fully responsible for such an action, and therefore these cases will not be considered in this article.

As more automobile security issues are reported, more lawsuits are being filed to determine the degree of legal liability that global automakers should take, which may lead to devastating corporate risks such as reputation damage and costly auto recalls and compensations. In this section, we will review some representative lawsuits and cases to explore the legal clauses for determining an automaker’s liability regarding vehicle malfunctions and security issues. We will also review some cases where recalls regarding security issues were spontaneously offered by automakers.

3.2.1 P. Spisto v. Toyota (2011) [14]

Spisto filed a lawsuit for vehicle defects and an accident against Toyota in 2007, when his Toyota vehicle accelerated of its own accord, went off the road, and crashed into a tree beside the road. Spisto was severely injured and burned by a fire from this accident. Since 2002, unintended acceleration as a result of a defective electronic throttle control system (ETCS) has been raised as an issue with Toyota's vehicles. Additional defects such as the absence of a brake override system, which prevents the vehicle from making arbitrary stops or decelerating, and a faulty gas pedal design causing its entrapment by the floor mat were also reported. The legal risks from this lawsuit are listed in **Table 3**.

Table 3. Legal risks in Spisto v. Toyota case

Legal risks (Toyota)	Details
Negligence	- Although being aware of a flaw in the vehicle design causing risks of injury by out of control operation or sudden unintended acceleration (SUA), Toyota did not take appropriate protective measures, including testing or warning.
Strict Product Liability	- Unsafe vehicles caused by defects in the designing, manufacturing, or testing phase or from some specific parts, do not meet their objectives as goods. - Whether Toyota noticed or did not notice defects in the design or development phase, there were no warnings or instructions issued to consumers.
Breach of Implied Warranty of Merchantability	- Toyota's advertisement of the vehicle implied warranted safety and reliability as a means of securing the value of transportation. However, it was not provided properly because of defects, consumer risk exposure, etc.
Fraudulent Concealment	- Toyota was in the "dealer's superior position" to know the hidden defects in the vehicle. However, the defects were not disclosed even after being detected. - Even after the vehicle's defect was disclosed, Toyota attempted to conceal it fraudulently.

According to the settlement of the Spisto-Toyota lawsuit, Toyota spent approximately $3.1 billion, with $1.1 billion spent to recall 16 million vehicles, install a new safety device, and compensate the drivers.

3.2.2 H. Cahen, et. al., v. Toyota, Ford, GM (2015) [16]

Automobiles manufactured by Toyota, Ford, and GM utilize about 35 ECUs and communicate via CAN communication. The packets transmitted via CAN communication are broadcast to all of the ECUs, which are connected to their corresponding BUS, and these packets are received and processed when necessary. However, according to several studies, it has been impossible to identify and authorize the transmitter of the CAN packets, making CAN communication vulnerable to external threats such as hacking. These automakers were aware of this issue, but they nevertheless continued their sales while emphasizing the "safety" of the vehicles as their highest priority. After learning about these studies, Cahen and others made a claim to the automakers for free repairs and compensation based on the warranty statement, but the automakers refused, arguing that security defects are not covered by the warranty's failure and overhaul items, which triggered the lawsuit.

Table 4. Legal risks in Cahen, et. al. v. Toyota, Ford, GM case

Legal risks (Toyota, Ford, GM)	**Details**
Non-observance of warranty (Magnuson-Moss Warranty Act)	- Defendant violated the warranty that if any defects or breakdowns are detected in the vehicle, a free repair or exchange is acceptable. - Even if the contract was not made directly with the complete vehicle company but through the dealer, the warranty had to be established between the plaintiff and defendant, and thus had to be observed.
Breach of Unfair Competition Law	- Even though the defendant recognized the defect when the plaintiff bought the vehicle, the defendant did not provide a notice of functional defects in the ECU. - In addition, violating the Magnuson-Moss Warranty Act by refusing to repair and exchange defective parts in the CANBUS was also a violation of the Unfair Competition Law. *It is regarded as a violation of the Unfair Competition Law when an illegal, unfair, or fraudulent business action, or false advertising is conducted.
Breach of Consumers Legal Remedies Act (CLRA)	- The defendant did not disclose the defect in the vehicle's CANBUS and only promoted the good points and safety of the vehicle. - This can be considered to be deceiving the plaintiff with illegal business actions because the plaintiff could not judge whether the price of the vehicle was reasonable or not.
Breach of False Advertising Law	- The defendant advertised false information about the vehicle's safety, reliability, and functionality.
Insufficient guarantee of Implied Warranty of Merchantability	- The defendant implicitly guaranteed the functionality and safety of the vehicle, even if this was not mentioned in the warranty. However, there were no actions to improve the vehicle when defects were noticed in various studies.
Breach of Contract/Common Law Warranty	- The defendant violated the terms of the conditions of the warranty in relation to revising or improving defective parts or technical elements of the vehicle.
Fraud by Concealment	- The defendant intentionally concealed defects in the vehicle.
Insufficient Guarantee of Song-Beverly Consumer Warranty Act for Breach of Express Warranties	- The defendant violated the warranty because even though the seller repaired the vehicle a certain number of times, it was not completely fixed. Thus, the seller should have exchanged the vehicle or returned the purchase cost.
Insufficient Guarantee of Song-Beverly Consumer Warranty Act for Breach of Implied Warranty of Merchantability	- The defendant notified the plaintiff of the merchantability of the vehicle. However, the vehicle had many security defects and did not meet this quality standard. *The defendant's vehicle should have had no defects, as mentioned in the contract, and the vehicle had to be designed and manufactured based on the purpose of use. In addition, the vehicle's functions and safety also has to be stated and ensured, as in the contract.

By analyzing the lawsuits and cases listed above, we found the types of corporate legal risks that may rise from automobile security defects and threats.

Table 5. Types of Legal Risks in Vehicle Development Phase

Paul Spisto v. Toyota	Cahen et.al v. Toyota, Ford, GM	Legal Risks	Phase
Strict Product Liability	-	Includes the risks mentioned below	Design /Develop
Breach of Implied Warranty of Merchantability	Implied Warranty of Merchantability	Breach of implied/express warranties for merchantability of the vehicle, not complying with related warranties	Sales
	Song-Beverly Consumer Warranty Act for Breach of Express Warranty		
	Song-Beverly Consumer Warranty Act of Implied Warranty of Merchantability		
	Magnuson-Moss Warranty Act		
	Contract/Common Law Warranty		
Fraudulent Concealment	Fraud by Concealment	Deceiving consumer, false advertising	
Negligence	False Advertising Law		
-	Consumers Legal Remedies Act		
-	Unfair Competition Law	Concealing defects, false advertisement, not complying with the warranty	Implement /Management

3.2.3 Fiat-Chrysler recall (2015)[17]

The "Uconnect dashboard," which is a driver convenience system built on a Sprint mobile network, is installed in some of the Fiat-Chrysler vehicle models. Security experts Miller and Valasek discovered critical weaknesses in their software for remote wireless control of the dashboard, steering wheel, transmission, and brake system, which led to a large recall. The number of recalled vehicles was around 1.4 million, and took the form of a software download from the internet and patch installation via USB, as well as an auto service agency visit.

3.2.4 Volkswagen emissions scandal (2015)[18]

Volkswagen intentionally manipulated the software of the emissions control systems installed in four diesel models manufactured since 2008, which was approximately 482,000 vehicles, to cheat on the US Environmental Protection Agency (EPA) emission tests. The software reduced emissions during the lab test, but emitted substances that were 40 times more toxic during actual driving on roads. Because of this scandal, Volkswagen's stock price dropped about 20% ($20 trillion in total), and they were expected to pay up to $18 billion in fines, and

even face class actions and indemnification claims. As can be seen from the intended fraud and concealment by an insider, Volkswagen's case is a good example of inappropriate management of security and the lack of internal compliance, and shows how much risk involving extra cost and reputation damage a corporation can face as a consequence.

4. Measures for risk management regarding connected car security issues in development process

The US government and council are making efforts to set up appropriate measures to regulate the automobile industry because of the rising concerns about automobile security issues. After the Fiat-Chrysler case, US senators Edward Markey and Richard Bluementhal proposed "The Security and Privacy in Your Car (SPY Car) Act" to enhance automobile security and protect privacy, and they are also pushing the US National Highway Traffic Safety Administration (NHTSA) and the Federal Trade Commission (FTC) to prepare an automobile security guideline based on this act. Below is a summary of the SPY CAR Act [2].

Table 6. Summary of SPY CAR Act of 2015

Category		Details
1	Cybersecurity Standard	**- Protection from hacking** · All motor vehicles should establish protection mechanisms against cyber attacks · The core software and systems should be isolated from other system areas · A vulnerability assessment of the above items should be conducted · Continuous security management/updates based on the results of the vulnerability assessment should be conducted **- Securing collected information** · Data stored in vehicles/external storage, or data transferred to other locations, should be protected from unauthorized access, etc. · Every motor vehicle must establish functions at the entry point to detect, report, and stop attempts to intercept driving data or control the vehicle
2	Privacy Standard for Motor Vehicles	**- Transparency** · Every motor vehicle should provide a notice in clear, plain language to the driver (owner) that the vehicle collects, transmits, retains, and uses driving data **- Consumer Control** · All drivers shall be given the option of terminating the collection and retention of driving data **- Limitation on Use of Personal Driving Information** · Manufacturers may not use any information collected by a motor vehicle for advertising or marketing purposes without affirmative express consent by the owner

3	Cyber Dashboard	- All motor vehicles manufactured for sale in the U.S. shall display a "cyber dashboard" as a component of the label required to be affixed to each motor vehicle

While regulations are being prepared to deal with automobile security issues, automakers should make spontaneous efforts to be more liable by abiding by the regulations and reducing legal risks. These spontaneous efforts may include installing or incorporating security technologies to prevent external hacking threats in the automobile design, development, sales and implementation/management stages, and establishing safety management procedures. In this section, we propose a security enhancement plan for the automobile development process from technical and operational perspectives.

Table 7. Security Responsibility Enhancement Plan and Related Parties

Process	Plans to Enhance Responsibility	Responsible Parties		
		Complete Vehicle Manufacturer	Parts Manufacturer	3rd Parties
Design /Develop	- Check security vulnerabilities	√	√	√
	- Secure management of supply chain	√	√	
	- Eliminate defects in software functions	√	√	√
Sales	- Renew warranties of electronic control systems	√		
Implement /Manage	- Delete sensitive data stored in scrapped vehicles or used cars/parts		√	√
	- Provide security updates for the electronic control systems of defective vehicles (or recalled vehicles)	√	√	√
	- Monitor security vulnerabilities continuously	√	√	√

4.1 Design and development stage

Today, the airbags, fuel supply system, ABS, AWD, GPS, and self-diagnostic devices that are installed in automobiles contain electronic parts. Because the relative proportion of such electronic parts in the software of automobiles has grown from 19% in 2014, to more than 40% in 2015 [19], the structure inside a vehicle is becoming more complex.

ISO26262 has recently been adopted to test for functional defects in the software installed in automobile electronic parts and guarantee safety. However, it is not suitable for testing for self-security weaknesses and external hacking because it is based on software error and failure tests. Therefore, procedures and methodologies must be prepared to check for vulnerabilities to potential external attacks, which may utilize various routes and security weaknesses in the source code. Automakers, parts suppliers, and other application and communication companies should regularly and spontaneously examine such possibilities.

Furthermore, a process for monitoring the appropriateness of the supply and distribution of auto parts should also be established. As of 2014, there were approximately 880 domestic auto parts suppliers [20], and their distribution network is extremely complicated. When new/used cars and genuine/non-genuine parts are considered separately, the distribution network becomes even more complex. Thus, it becomes difficult to detect and track software forgery or modification. Therefore, automakers should establish a supply chain security management system to track the records of electronic control part forgeries or modifications by auto part suppliers, sales agencies, and repair shops, which may occur during the manufacturing or supply processes, and to keep track of the detailed history of weakness test reports.

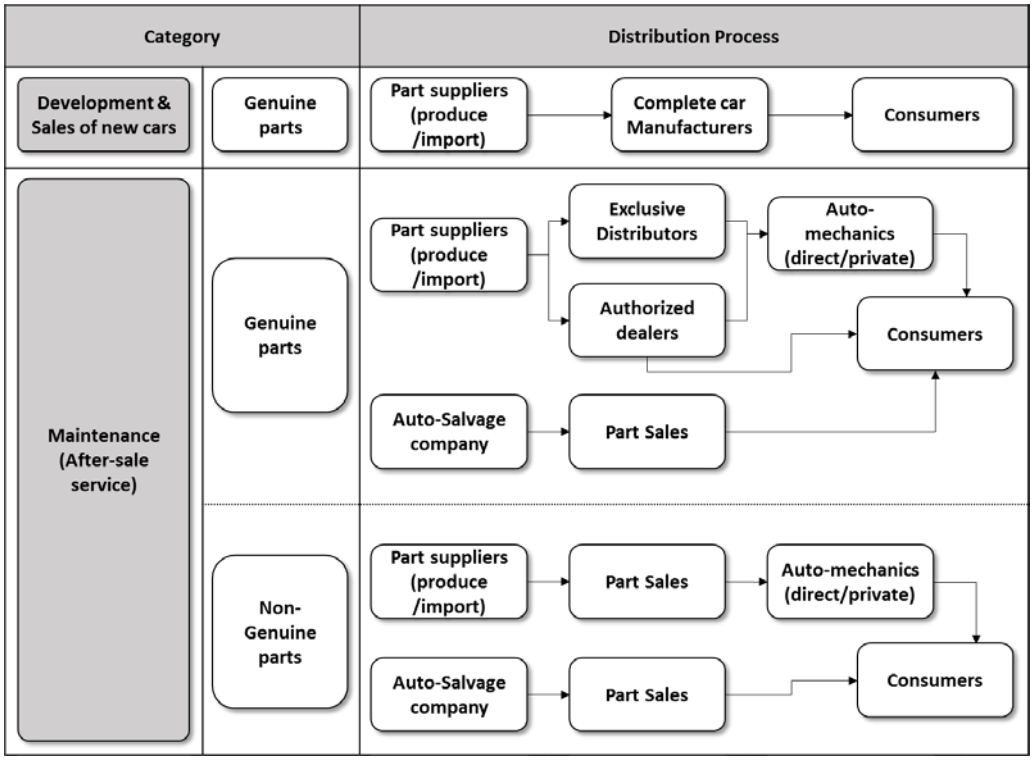


Fig. 5. Supply chain for new/used parts of vehicles

4.2 Sales stage

The warranty policies for automobiles, which are sold to customers by automakers, primarily specify the warranty periods and terms for consumable parts such as tires and spark plugs. Because newly released vehicles are evolving into connected vehicles, most of today's vehicles are loaded with a variety of sensors and electronic control devices. However, the terms and conditions of an automobile's warranty do not specify any clear scheme for security problems. Thus, the issue of unclear responsibilities and legal issues regarding automobile security are being raised. Therefore, it will be crucial to set up a standardized policy that explicitly specifies security weakness reviews for electronic control devices such as ECUs, and a software patch warranty to solve problems regarding vehicle malfunctions caused by external factors such as hacking.

Table 8. Global automobile companies' warranties on ECUs

Company	Terms and Conditions of the Warranty	Express Warranty on ECU
A	- Basic parts (except tires, unwired headphones, parts added or modified after delivery), corrosion, powertrain, etc.	X
B	- (general vehicle) bumper-to-bumper, powertrain, safety restraint system, corrosion, powerstroke diesel engine, etc.	X (OBD related to emissions, ECC sensors, switches, ECMs are guaranteed)
	- (hybrid electronic vehicle) bumper-to-bumper, powertrain components, safety belts, SRS, corrosion, hybrid/electric components, etc. (no warranties for S/W modification–but no mention of vicious modifications)	X
C	- Bumper-to-bumper (including tires), engine, powertrain components, transmission, drive systems, etc. (sensors, wiring, connectors, control module and module programming for engine/powertrain/transmission and driving systems are not included)	X
D	- Basic parts (powertrain-engine, transmission and transaxle, front/rear wheel drive system), restraint system, corrosion perforation, towing, emission defect/performance, air/fuel metering system, air induction system, catalyst system, evaporative control system, etc. - Other parts used in above systems (data link connector, sensors, switches, valves, etc.)	X

4.3 Implementation/management stage

Today, the ECUs of scrapped vehicles are often traded as second-hand products and reused for the sake of environmental protection and cost saving. These reused ECUs must be checked for any customization by the original user that could make the ECU vulnerable, or any sensor information and diagnostic trouble codes (DTC) that might remain in electronic control devices. Furthermore, procedures and measures should be established to check whether personal information such as driving information, images, and video clips stored in the built-in memory of infotainment devices such as an automobile's GPS and AV systems.

As more electronic control devices are utilized for vehicle convenience and safety, recalls due to S/W vulnerability and defects are expected to rise continuously. The length of the S/W code installed in vehicle electronic control devices can range from 20 or 30 million lines to 100 million lines. Given that the S/W recalls occurring in the North American/European automobile industry make up 60% to 70% of the entire recalls, and assuming that one line of code costs an average of $10, the total expense for a recall can be astronomical [23]. Therefore, measures for the efficient distribution and application of electronic control device security patches must be established to reduce the risk of the extra cost that may arise from recalls and security defects.

Table 9. Recent recall cases of global automobile companies

Category		Reasons for recall	Amounts
Jul. ’15	Fiat Chrysler	S/W patches for security vulnerabilities	1,400,000
May ’14	Ford	S/W updates for airbags and transmission control	695,000
Jul. ’15	Ford	S/W updates for vehicle stalling	430,000
Jul. ’15	Land Rover	S/W bug updates for locking systems	65,000
Jul. ’15	Toyota	S/W updates on electronic control systems for motor, engine generator	109,000
Feb. ’14	Toyota	S/W updates for hybrid control units	1,900,000

Finally, automakers, auto part suppliers, and other players must establish a system that is capable of continuously monitoring novel IT and information security issues, as well as vehicles, to make it possible to share information and react whenever vulnerabilities are discovered.

5. Conclusion

In today’s “connected” environment, vehicles are loaded with numerous electronic control devices, and various sensors are connected to each other via wired/wireless communication, which leads to different types of security defects and vulnerabilities to external hacking attacks. Based on the previously discussed relevant cases, an automaker’s passive technical/administrative response to functional errors or security issues in vehicles can lead to massive expenses from large-scale recalls or indemnifications and corporate reputation damage risks, which could ultimately lead to a national level loss, given the uniqueness of the automobile industry. The United States government is preparing national-level solutions such as drafting a bill or setting up a guideline for government organizations to handle automobile security issues. Various other countries have also become aware of automobile security issues and are making relevant efforts.

In this article, we considered cases in which legal liability was brought up as a result of security issues within the automobile environment, which is continuously moving toward being “connected.” Security requirements were proposed for each process, including the automobile design/development, sales, and implementation/management stages, to strengthen the responsibilities of automobile industry players and allow them to properly handle such potential security risks.

At the design/development stage, potential automobile security weaknesses and S/W functional defects should be analyzed in advance, and protective measures should be taken. Forgery and modification should be prevented, and follow-up control should be carried out by keeping track of electronic communication parts and supply histories. At the sales stage, the service policy should be amended so that the patch support, maintenance, and overhaul of electronic control devices such as ECUs, AVNs, sensors, and communication interfaces can be efficiently provided. This will make it possible to actively respond to any potential security issues that may arise during the evolution toward a “connected” vehicle environment and explicitly ensure safety against hacking threats. At the implementation/management stage, the continuous monitoring of novel security threats that may arise in the parts loaded in automobiles and S/W must be carried out. In addition, when previously unknown weakness or security defects are discovered, patches should be distributed and applied according to the explicit coverage of the policy. In addition, an appropriate procedure must be established to

check whether sensitive information is deleted, and whether there is any S/W forgery or modification when used vehicles and related parts are traded.

Regarding various legal risks of security issues that may arise in the automobile-based IoT industry, the responsibilities of companies must be stressed, and national-level automobile security regulations are necessary. Thus, an appropriate guideline should be developed. We believe that this article can make significant contributions in this respect, by providing directions for automakers to develop detailed policies and strengthening their responsibilities to reduce legal risks from security problems. Future work should analyze various cases dealing with the security issues of the IoT and related industries (e.g., smart homes and smart medicine). Then, based on this study, research should be performed on the development of national-level security guidelines and a spontaneous corporate responsibility enhancement framework.

References

[1] Broy. M. et. al., "Engineering Automotive Software," in *Proc. of the IEEE*, vol. 95, no. 2, Feburary, 2007. Article (CrossRef Link)

[2] ED Markey, "SPY Car Act of 2015" Article (CrossRef Link)

[3] Paul T. Durbin, *Critical perspectives on nonacademic science and engineering*, Lehigh University Press, 1991.

[4] Shirley Radack, *THE SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)*, National Institute of Standards and Technology (NIST), 2009. Article (CrossRef Link)

[5] *ISO/TS 16949:2009 Quality Management Systems*, International Organization for Standardization, 2009.

[6] *Advanced Product Quality Planning(APQP)*, 2nd Edition, Automotive Industry Action Group (AIAG), July, 2008. Article (CrossRef Link)

[7] *ISO 26262-6:2011 Part 6: Product development at the software level*, International Organization for Standardization, 2011.

[8] I. Rouf et al., "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study," USENIX Security '10, in *Proc. of the 19th USENIX conference on Security*, 2010. Article (CrossRef Link)

[9] S. Checkoway, et. al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," *USENIX Security Symposium*, 2011. Article (CrossRef Link)

[10] Tyagi, et. al., "Investigating the security threats in Vehicular ad hoc Networks (VANETs): Towards security engineering for safer on-road transportation," in *Proc. of Computing, Communications and Informatics* (ICACCI), 2014 International Conference on IEEE, 2014. Article (CrossRef Link)

[11] J. Petit, S. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Transactions on Intelligent transportation systems*, vol. 16, no. 2, April, 2015. Article (CrossRef Link)

[12] *An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues*, U.S. Department of Transportation (RITA), November, 2011. Article (CrossRef Link)

[13] *A Survey of Remote Automotive Attack Surfaces*, IOActive, 2014. Article (CrossRef Link)

[14] Paul Spisto, et al., v. Toyota Motor Corporation, U.S. District Court of Central California, Civil Action Case No. CV11-04479CBM(RZx)

[15] *Toyota in $1.1 Billion Gas-Pedal Settlement*, The Wall Street Journal, Dec. 27, 2012. Article (CrossRef Link)

[16] Cahen, et al. v. Toyota Motor Corporation, et al., U.S. District Court of Northern California, San Francisco Division, Civil Action No. 4:2015cv01104.
[17] *Regulators Investigating Fiat Chrysler Cybersecurity Recall*, The Wall Street Journal, Jul. 24, 2015. Article (CrossRef Link)
[18] *Volkswagen's Emissions Scandal*, The Wall Street Journal, Sep. 21, 2015. Article (CrossRef Link)
[19] *The Motor Vehicle Supply Chain: Effects of the Japanese Earthquake and Tsunami (Congressional Research Service 7-5700)*, Bill Canis, May. 23, 2011. Article (CrossRef Link)
[20] Korea Auto Industries Coop. Association (KAICA), Article (CrossRef Link)
[21] *A Survey on Distribution of Spare Parts for Vehicle (No. 10-05)*, Korea Consumer Agency (KCA), May, 2010.
[22] *A Study on Distribution for After-Sales Vehicle Parts and Promoting Competition in Mechanic Field*, Fair Trade Commission (FTC), Sep. 30, 2002.
[23] *Over-the-Air Updates to Slash Automobiles' Recall Rates*, Finds Frost & Sullivan, PR Newswire, September, 2013. Article (CrossRef Link)
[24] *Caution: Malware Ahead, An analysis of emerging risks in automotive system security*, McAfee, 2011. Article (CrossRef Link)
[25] I. Kruger, "Improving the Development Process for Automotive Diagnostics," in *Proc. of 2012 International Conference on Software and System Process (ICSSP)*, pp.63-67, June, 2012. Article (CrossRef Link)
[26] *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, ED MARKEY, Feburary, 2015. Article (CrossRef Link)
[27] W. B. Jaballah, M. Conti, M. Mosbah, C. E. Palazzi, "Fast and Secure Multihop Broadcast Solutions for Intervehicular Communication," *IEEE Transactions on Intelligent Transportation Systems*, Vol.15, No.1, pp.433-450, 2014. Article (CrossRef Link)
[28] G. Calandriello, P. Papadimitratos, J. P. Hubaux, A. Lioy, "On Performance of Secure Vehicular Communication Systems," *IEEE Transactions on Dependable Security Computing*, Vol.8, No.6, pp.898-912, 2011. Article (CrossRef Link)

Dong Hee Kim is a Ph.D. candidate in the Graduate School of Information Security at Korea University and a senior researcher at the National Security Research Institute. He received his M.E. in Information Security Policy from Korea University. His primary research area is the National Cybersecurity, Information Security Policy, Security of Converging Technologies and Cyber Warfare.

Seung Jo Baek is a research professor of the Center for Information Security Technologies (CIST) at Korea University, a director of the Center for Cyber Security Policy (CCSP) and a principal research engineer of the Cyber Defense Research Center (CDRC) at Korea University. He received his M.E. and Ph.D. degrees in Information Security Policy from Korea University. His primary research area is the National Cybersecurity Policy, International Cybersecurity Cooperation, Privacy Protection, Cyber Peace and Human Rights.

Jongin Lim is a professor of the Graduate School of the Information Security/Department of the Cyber Defense in Korea University. He received B.S., M.S., and Ph.D. degrees in the Department of Mathematics at Korea University. He is a former Special Advisor to the President for National Security, Republic of Korea. His primary research area is National Cybersecurity, Information Security Policy, Cyber Warfare, Security of Converging Technologies, Privacy and Cryptography.