

Security Threat Analysis for Remote Monitoring and Control Functions of Connected Car Services

Jin Kim¹ and Jinho Yoo^{2,*}

Abstract

The connected car services are one of the most widely used services in the Internet of Things environment, and they provide numerous services to existing vehicles by connecting them through networks inside and outside the vehicle. However, although vehicle manufacturers are developing services considering the means to secure the connected car services, concerns about the security of the connected car services are growing due to the increasing number of attack cases. In this study, we reviewed the research related to the connected car services that have been announced so far, and we identified the threats that may exist in the connected car services through security threat modeling to improve the fundamental security level of the connected car services. As a result of performing the test to the applications for connected car services developed by four manufacturers, we found that all four companies' applications excessively requested unnecessary permissions for application operation, and the apps did not obfuscate the source code. Additionally, we found that there were still vulnerabilities in application items such as exposing error messages and debugging information.

Keywords

Connected Car, Security, Threat Modeling, Vulnerability Analysis

1. Introduction

In the current rapidly changing digital environment, the Internet of Things (IoT) has become a core requirement for next-generation computing, and network functions are being added to most existing and newly launched products. Individual products are connected to form a large network through a network and provide new services through the interactions between products and users. The concept of connectivity has emerged, and as the data and information of products change the competitive landscape and industry definition, it is changing into a new type of competitive environment. “Connected car services” can be called one of the representative connected services at the center of these changes.

The connected car services are creating new business opportunities through real-time fault diagnosis or real-time response for vehicle safety [1,2]. Ford uses location-based information to provide drivers with real-time traffic conditions, which can be used for road guidance, and provides services that allow users to enjoy various entertainment through cloud-based contents inside the vehicle [3]. Since the feasibility of the connected car services revenue model has been verified, interest in the connected car services is growing [4].

※ This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Manuscript received November 6, 2023; first revision January 9, 2024; accepted March 6, 2024.

*Corresponding Author: Jinho Yoo (jhyoo@smu.ac.kr)

¹ Big Data Convergence Major, Sangmyung University, Seoul, Korea (jinkim@smu.ac.kr)

² Division of Business Administration, Sangmyung University, Seoul, Korea (jhyoo@smu.ac.kr)

With the increasing interest in connected car services, there are concerns regarding the adequacy of security preparations for securing them. Attackers already view automobiles as new targets for attacks, and if they are compromised, they are expected to pose a significant risk. Therefore, in this paper, we aim to identify security threats to connected car services and analyze security vulnerabilities.

2. Related Work

2.1 Connected Car

Recently, the term “hyper-connected society” has been used frequently. Hyper-connected society refers to an environment in which people, objects, and spaces are all connected through networks and in which information is created or collected, shared, and utilized. It is expected for the future to change significantly due to the IoT and artificial Intelligence (AI), which are digital technologies that continue to develop in a hyper-connected society [5].

A connected car is a vehicle that is connected to a network and provides various services, including autonomous vehicles and smart cars. By using a connected car, it is possible to provide services such as remote start and remote diagnosis of the vehicle, telephone, message transmission and reception, e-mail transmission and reception, real-time traffic information confirmation, and emergency rescue through the network with the inside or around the vehicle. Drivers can drive comfortably using a connected car connected to the network. The main functions of a connected car include a mobile management function that allows drivers to reach their destination safely and quickly, a vehicle management function that reduces operating costs and adds convenience to operation, an entertainment function that provides entertainment to the driver and passengers, and an in-vehicle and There are a safety function that notifies the driver of external dangers, and a driver assistance function that enables partially autonomous driving, and a well-being function that provides comfort to the driver [6].

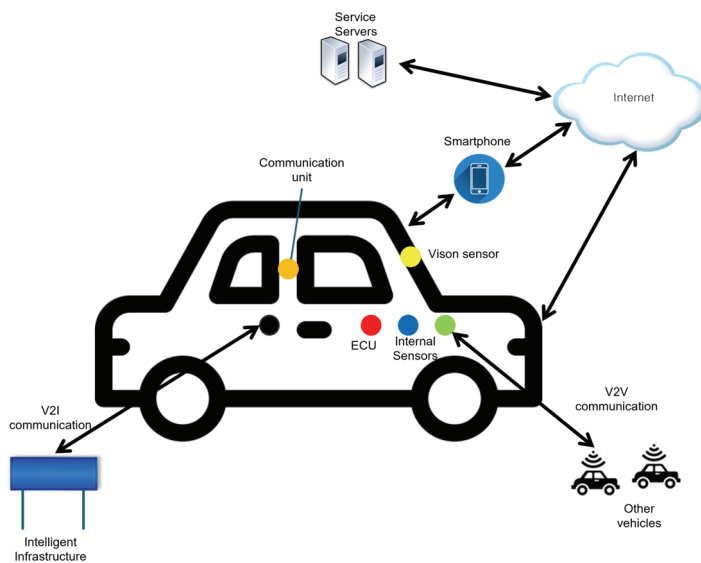


Fig. 1. Overview of the connected car system.

The connected car is an evolution of past telematics technology and is related to machine-to-machine communication and intelligent transportation system technology (Fig. 1). Telematics uses information communication technology technologies, including networks, to provide services such as vehicle location tracking, Internet connection, remote vehicle diagnosis, remote accident detection, and traffic information [7,8]. In addition, in-vehicle telematics is being advanced in line with the recent development of communication technology, including IoT [8].

The connected car services are expected to evolve into a convergence service where network functions are improved, infotainment functions are expanded, and communication services are strengthened. It executes the optimization algorithm and transmits it to the maintenance team and driver to perform vehicle diagnosis and regular inspection, saves fuel economy, provides a driving guide, and is expected to develop into an autonomous vehicle.

2.2 Threat Modeling

The purpose of threat modeling is to use a model to find security problems in a product or a service. Threat modeling has existed in the past, but it has been studied in earnest since the 1990s. In general, when performing security threat analysis using threat modeling, the product is analyzed first, the threat is identified, the attack tree is created, and then the vulnerability checklist is derived in this order. Researchers usually create an Attack Library that collects previously known vulnerabilities to derive an attack that can occur from each threat, and they work with reference to this Attack Library [9,10] (Table 1).

Table 1. Types of threat modeling [9,10]

Name	Description
UML (unified modeling language)	Visually represent those systems and as a result
Misuse Case	Describes features the system cannot allow
Threat Tree	Identify how and under what condition threats can be realized
Attack Tree	The tree root is the goal for the attack, and the leaves are ways to achieve that goal
STRIDE	Identify all potential threats within a system and the specific properties being violated
LINDDUN	Provides a systematic approach to privacy assessment
OCTAVE	Focuses on organizational risks and not technological risks
TVRA	Identify risk to the system based upon the product of the likelihood of an attack
PASTA	Employs an attacker-centric perspective to produce an asset-centric output
Trike	Security auditing framework that turns a threat model into a risk management tool






STRIDE is an acronym for potential security vulnerabilities. It stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [11]. LINDDUN is one of the threat modeling methods, primarily used for analyzing threats to personal information. LINDDUN consists of the first letters of six properties: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance.

3. Security Threat Modeling for Connected Car Services

3.1 Structural Analysis using DFD

In this paper, STRIDE and LINDDUN are used to identify threats in terms of software and privacy. For this, a detailed analysis of key components, including entities, processes, data stores, and data flows, is required. Data flow diagram (DFD) is performed as one step in the process of security threat modeling, allowing for an overview of the data flow. The expression rules for DFD are shown in Table 2.

Table 2. Symbols of data flow diagram

Element	Symbol	Description
Trust boundary		Boundary between trust levels or privileges
Entity		Interact with the system
Data store		Repositories of data
Process		Transforms incoming data flow into outgoing data flow
Data flow		Data packet flowing from one process to another process

Connected Car Services include entities such as the user, smartphone, manufacturer server, app store server, vehicle edge, and Engine Control Unit (ECU). Since the type of conceptual data transferred between entities is expressed in the context diagram, it is possible to understand how the entire services are composed and the flow of core data. However, it does not provide an understanding of the internal workings of the analysis target. DFD is created based on the context diagram, and the main process is explained in more detail as the level rises to Level 0, Level 1, etc. The final DFD creation result for the Connected Car Services is shown in Fig. 2.

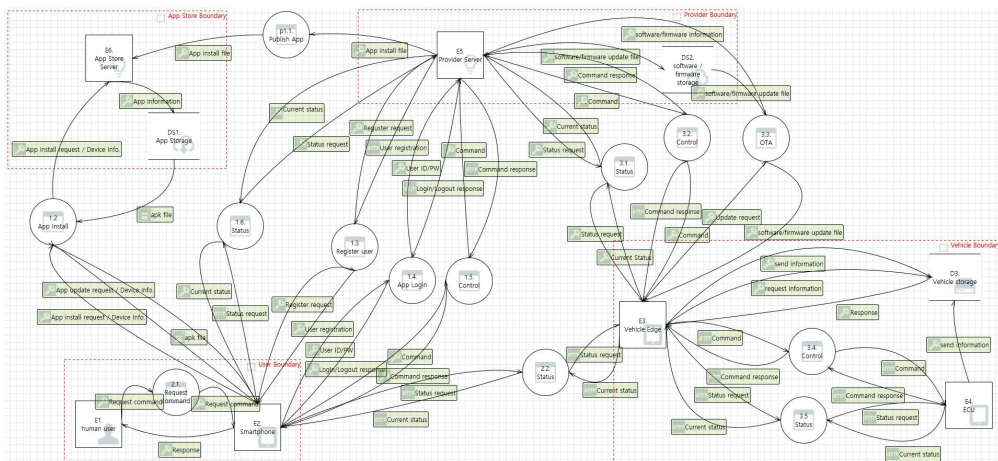


Fig. 2. Final data flow diagram of connected car services.

3.2 Collect Attack Library

Attack Library is created to determine whether properly identifying threats that may arise from each item of the DFD created in Section 3.1. Attack Library is created by collecting various types of data such

as papers, conferences, technical documents, common vulnerabilities and exposures (CVE), and international standards. The vulnerabilities and attack methods of the connected car services, the subject of this study, are classified into applications, networks, systems, and hardware. Attack Library was prepared by referring to these, technical documents, CVEs, and security conferences. The attack library collected for this study is shown in Table 3 [12-17]. Through the creation of the Attack Library, the threat to the analysis target can be detailed, and all known attack routes, types, and methods so far can be identified.

Table 3. Attack Library sample of connected car services

No.	Type	Category	Title	Author	Threat
1	Technical document	All	Intelligent vehicle security threats and countermeasures report	Institute of Information & communications Technology Planning & Evaluation [12]	STRIDE
2	Paper	Network	A brief survey on autonomous vehicle possible attacks, exploits and vulnerabilities	Kumar et al. [13]	T
3	Conference	Hardware	Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study	Roufa et al. [14]	I
4	Paper	Hardware	Revisiting attacker model for smart vehicles	Petit et al. [15]	I
5	Paper	Network	Remote attacks on automated vehicles sensors: experiments on camera and LIDAR	Petit et al. [16]	SD
6	Conference	Network	Experimental security analysis of a modern automobile	Koscher et al. [17]	I

3.3 Threat Identification with STRIDE

When I checked all the processes of the connected car services in detail, I checked a total of 52 components. Each component contains a potential threat. Using STRIDE, one can identify the threat of each component. At this time, for accurate and consistent threat identification, the threat is identified by referring to the Attack Library created in Section 3.2. Table 4 shows the results of STRIDE analysis for each element.

As a result of STRIDE analysis, a total of 99 threats were found in the connected car services. Among them, Tampering and Information Disclosure were identified as the primary threats, while Spoofing (disguised as a normal user) and Elevation of Privilege (acquiring administrator rights) were relatively less common. This seems to be because the connected car services offer a generic service that can be used by various users instead of offering user-specific services through user identification or authentication. The STRIDE analysis result is a list of threats that can occur in the connected car services, and it is necessary to use the Attack Library and Attack Tree to check which attacks can occur due to these threats.

3.4 Attack Tree

In Attack Tree, an attack target is named as a root node, and detailed attack methods to carry out the attack are created as sub-nodes. There are four types of attacks that are used in the connected car services. They are data acquisition, data tampering, administrator privilege (shell) acquisition, and denial of service. Most attacks are generated by tampering with firmware or executing malicious applications (Table 5).

Table 4. STRIDE analysis result sample of connected car services

Entity No.	Name	STRIDE	Threat definition	Threat No.
E1	User	S	The attacker pretends to be someone else with malicious intent	T1
		R	Attacker denies manipulating connected car service app	T2
E2	Smartphone	S	Attacker poses as an authorized user to manipulate app data	T3
E2	Smartphone	T	Tampering with memory, files on a smartphone	T4
E2	Smartphone	R	Deny accessing the smartphone's memory, files, etc.	T5
E2	Smartphone	I	Exposing the memory and file contents of your smartphone	T6
E2	Smartphone	D	Failed to provide service due to memory corruption	T7
E2	Smartphone	D	Failed to provide service due to network load	T8
E3	Vehicle edge	T	OBD port vulnerabilities	T9
E3	Vehicle edge	I	OBD port vulnerabilities	T10
E4	ECU	S	Camouflage ECU	T11
E4	ECU	E	Granting access without valid authorization	T12
E4	ECU	S	Bypassing authentication	T13
E4	ECU	T	Buffer overflows	T14
E5	Provider server	S	Attacker masquerading as a manufacturer's server	T15
E5	Provider server	R	Deny sending/receiving data	T16
E5	Provider server	D	Service outage due to network resource exhaustion	T17
E6	App store server	S	Attacker masquerading as an app store server	T18
E6	App store server	R	Deny sending/receiving data	T19
E6	App store server	R	Deny access to server	T20
E6	App store server	D	Service outage due to network resource exhaustion	T21

Table 5. Attack Tree sample of connected car services

	Attack target		Threat	
1	Obtain administrator privileges (shell)		-	
OR	1.1	Executing malware	-	
	OR	1.1.1	Executing malicious applications	
		OR	1.1.1.1	
			Tampering with existing applications	T14, T15, T18, T22, T23, T31, T32, T34, T35, T37, T53, T57, T58, T59, T61, T63, T64
		OR	1.1.1.2	
			Installation of malicious applications	T14, T15, T18, T22, T23, T31, T32, T33, T34, T35, T36, T37, T53, T57, T58, T59, T60, T61, T62, T63, T64
	OR	1.1.2	Executing malicious scripts	-
		OR	1.1.2.1	
			Accessing malicious web pages	T3, T4, T14, T15, T18, T53
		OR	1.1.2.2	
			Executing malicious script file	T3, T4, T14, T15, T18, T53
	OR	1.1.3	Executing malicious software	-

3.5 Threat Identification with LINDDUN

We identified threats related to personal information of the connected car services using LINDDUN, which is advantageous for privacy-focused threat identification. Unlike STRIDE, LINDDUN builds a Threat Tree for each possible threat. The analysis result by applying LINDDUN to the DFD element of the connected car service is shown in Table 6.

Table 6. LINDDUN analysis result sample

Element	No.	Title	L	I	N	D	D	U	N
Entity	E1	User		×				×	
	E2	Smartphone		×				×	
	E5	Provider server		×				×	
Data store	DS1	App store	×			×	×		
	DS2	Software/Firmware storage	×	×			×		×
	DS3	Vehicle edge	×	×		×	×		×

As a result of detailed LINDDUN analysis, most threats were related to Detectability, that could potentially reveal a user's interests, preferences, or tastes, rather than Identifiability, which can identify a user's identity from personal information in connected car services. This is because the portions of authentication and identification in the connected car services are not as large as the result of STRIDE analysis in Section 3.3, so there is not much data that can identify the user's identity. In addition, we can know that there is a lot of data that could potentially reveal interest items, tastes, dispositions, and personalities, which can be analyzed based on the behavior patterns or behaviors of connected car services users.

3.6 Threat Tree

When threat identification for each component of DFD is completed using LINDDUN, a Threat Tree is created that identifies detailed information for each threat related to each item. Table 7 is the Threat Tree of the Entity.

Table 7. Entity Threat Tree sample

Identifiability	
1	I_E
1.1	I_E1: Login using an untrusted method
1.1.1	I_E4: An identifiable login method.
1.1.1.1	I_E9: Use real identity information to login
1.1.1.2	I_E10: Use a pseudonym to log in
1.1.1.2.1	I_E12: Use ID and password
1.1.1.2.1.1	I_E14: Existence (first name, last name, etc.) of an association between the ID and an identity

3.7 Misuse Case

In order to help the understanding of the created Threat Tree, a Misuse Case (MUC) is created based on the scenario. The MUC is written to include all the contents of the Threat Tree, which includes the identifier, summary, main attacker, scenario, and the results of the Threat Tree related to the MUC. Table 8 is the MUC based on the Threat Tree.

As a result of analyzing the Threat Tree, a total of 15 MUCs have been derived. As a result of checking 15 MUCs, cases for Identifiability and Unawareness have been derived for Entity, and cases for Linkability, Identifiability, Detectability, Disclosure of Information, and Non-Compliance have been derived for Data Store, Process, and Data Flow. Through this, it is judged that the Data Store, Process, and Data Flow share similar vulnerabilities.

Table 8. MUC sample for Threat Tree

MUC	Description
MUC 01	<p>The corresponding tree : I_E</p> <p>Summary: A problem with the smartphone, server, vehicle, or network could expose someone's identity to unauthorized parties.</p> <p>Main attacker: Insider-outsider with attack capabilities</p> <p>Scenario:</p> <ol style="list-style-type: none"> s1. Vulnerabilities in login forms could allow attackers to identify users' identifying information from data. s2. When you sign in, use data associated with your real identity. s3. When logging in, use data (username, password) that can be inferred from real identity. s4. When logging in, a vulnerable software token is used. s5. User's information is exposed through a malicious application. s6. User's information is exposed because the user was given an untrusted device. s7. Information is exposed due to a lack of Confidentiality for transmitted or received data. s8. Information in a network channel or Data Store is exposed, or data is exposed due to Linkability. <p>Result: The information obtained can be used to identify the user. The attacker can also use the user's identity to obtain new information or to distinguish the user from other users.</p>

4. Security Vulnerability Analysis of Connected Car services

4.1 Derivation of Checklist for Vulnerability Check

In this study, vulnerability checks are mainly performed on mobile apps for Connected Car Services. We decided that it would be appropriate for experts to perform a vulnerability analysis on a mobile app rather than relying on a commercial solution. Therefore, a checklist for vulnerability analysis was derived, and vulnerability analysis was performed on the list. The vulnerability checklist was prepared by referring to the “Mobile Public Service Security Vulnerability Check Guide” of Korea Information Security Agency, a guideline for mobile app vulnerability check. Among the threat items of the list derived by applying STRIDE and LINDDUN modeling, the checklist is composed of items that can be checked without affecting the vehicle. The vulnerability checklist was divided into three areas: application, network, and system (Table 9).

4.2 Security Vulnerability Analysis Result

As a result of the security evaluation of the connected car services by each manufacturer, it was confirmed that the development was carried out with security in mind, except for some items. The vulnerabilities found in the service are shown in Table 10. In the application section of the checklist, vulnerabilities were found in the authentication policy limit of the number of login attempts (A1) for one manufacturer service and the complexity of setting password rules (A2). In addition, all four manufacturers requested unnecessary permission for App operation (A5), and the communication data is encrypted through Secure Sockets Layer (SSL). However, Android Package (APK) source code obfuscation (A6) has not been applied, so it may be exposed to the risk of source code analysis for malicious purposes. In the network and system section, safety actions were taken by performing encryption and other proper actions, but company C and company D did not check whether the device is rooted (S4), so there was a threat that could be used for an attack through an emulator.

Table 9. Checklist for security vulnerabilities in connected car services

Category	Check Item	No.	Detail	Analysis method	Threat No.
Application	User authentication	A1	Check the number of sign-in attempts limit (3-5)	After running the mobile app, enter account information 5 times	T1, T3
		A2	Check password rule settings -Contains alphabets, special characters, and numbers -Consists of 8 or more characters in length	Make sure the password is set to be complex	T1, T3
		A3	Check personal information exposure	Check whether authentication-related information is sent over SSL	T39, T66, T69
		A4	Check for authentication-related information exposure Cookies, sessions, values, tokens, and more	Check whether authentication-related information is sent over SSL	T39, T40, T66
	Unauthorized accessibility	A5	Check for unnecessary permission requests for APP actions	Check for unnecessary permission requests for APP actions (Decompile using Apktool to verify)	T4, T14, T22, T31, T53
	Encryption	A6	Check APK source code obfuscation	Check whether the APK file source code is obfuscated using Apk Manager.	T4, T6, T29, T37, T53, T60
		A7	Whether communication data is encrypted	Check whether communication data is encrypted using WireShark	T52, T74, T79, T82, T86, T88
	Debugging	A8	Whether error messages and information are exposed	Check whether error messages are exposed using Logcat Filter	T4, T22
		A9	Whether debugging information is exposed	Check whether debugging information is exposed using Logcat Filter	T4, T22
Network	Port scanning	N1	Check open ports (dongles)	Check open ports using NMAP and web browser	T47, T49
		N2	Check unnecessary management ports	Check unnecessary management ports using NMAP and web browser	T47, T49
	Packet Sniffing	N3	Check whether sensitive information is encrypted	Check encryption of sensitive information using Burp Suite	T74, T79, T82
		N4	Obtaining sensitive information through man-in-the-middle attacks	Check encryption of sensitive information using Burp Suite	T74, T79, T82
	Packet transfer	N5	Check vehicle control by sending arbitrary commands	Check whether arbitrary commands are transmitted using Burp Suite	T74, T79, T82
		N6	Check for replay attacks	Check whether replay attack is possible using Burp Suite	T1, T3
System	System shell check	S1	Check for administrator ID/PW exposure in the system shell	Use ADB (Android debug bridge) to check whether ID/PW is exposed in installed internal files or among decompiled contents.	T39, T65, T66, T68
		S2	Check whether general users can access the administrator shell	Check whether general users can access the administrator shell using ADB	T4, T14, T22, T31, T53
	Information processing	S3	Check measures to de-identify personal information on the device (SQL)	Check personal information de-identification measures using ADB	T23, T24
	Tampering	S4	Check whether the device is rooted	Check whether you are rooted by installing the mobile app on NOX (emulator program)	T4, T6, T7

Table 10. Compare security vulnerabilities in connected car services

Item	Company A	Company B	Company C	Company D
Application	Unauthorized accessibility Encryption (source code obfuscation) Debugging	Unauthorized accessibility Encryption (source code obfuscation) Debugging	Unauthorized accessibility Encryption (source code obfuscation) Debugging	User authentication (limit the number of sign-in attempts, password complexity) Unauthorized accessibility Encryption (source code obfuscation) Debugging
Network	-	-	-	-
System	-	-	Tampering	Tampering

5. Conclusion

In this paper, we reviewed the research related to the connected car services that have been published so far and presented a security checklist through security threat modeling to improve the fundamental security of the connected car services. To derive an effective security checklist, DFD was derived from analyzing the data flow of the connected car services, and based on this, threats that could occur in the connected car services were identified using STRIDE and LINDDUN, the security threat modeling methodology. Afterwards, a checklist to remove the identified threats was derived. Using this, we performed the security vulnerability analysis of the connected car services.

As a result of analyzing apps developed by four manufacturers, all four companies excessively requested unnecessary permissions for APP operation, the source code was not obfuscated, and there were still vulnerabilities in the application section such as exposing error messages and debugging information. In addition, it was confirmed that there was a high possibility of being a target of an attack because some manufacturers' apps did not check if the devices were rooted.

STRIDE, a security threat modeling method for the software aspect, and LINDDUN, a security threat modeling method for personal information protection, were applied together to examine two aspects of security threats: the software aspect and personal information protection. In the case of existing papers related to security threat modeling, security threat modeling was mainly performed using one methodology, but it can be said that there is rarity in that both were applied together. We derived the security threat of the connected car services using the security threat modeling methodology, and we made a security checklist based on this. Car manufacturers should consider security aspects as well as service usage aspects in the planning stage of connected car services. If we use the checklist made through this study, the security aspect can be further strengthened.

The results of this study are expected to be used in various ways as follows. First, a threat model can be used to identify issues before developing software for connected car services. Second, it is expected that it will be helpful in effectively performing vulnerability analysis on connected car services in the future based on the identified security threats and checklists for vulnerability analysis to connected car services using threat modeling. Third, it is expected that the threat identification, checklist, and vulnerability analysis results presented in this paper can be used as an objective reference to consider in

terms of security when developing connected car services.

In this study, we conducted vulnerability tests on apps that can be controlled remotely, rather than on parts of connected car services that are directly connected to the vehicle. When conducting vulnerability tests on vehicles without the help of vehicle manufacturers, the scope of the test is necessarily narrowed due to the risks that may occur in the vehicle. In addition, when conducting penetration testing, it is usually performed with the knowledge of the operating organization of the target system. In the case of connected car services, we excluded them from the scope of our analysis because conducting vulnerability analysis on vehicle-related servers at random would place a significant load on the servers. In the future, it is believed that much more meaningful results can be obtained by including equipment such as vehicles and related servers in the scope of vulnerability analysis in consultation with vehicle manufacturers.

The scope of this study was limited to analyzing security threats to apps that focus on remote monitoring and remote-control functions in connected car services. It would have been more meaningful to identify the characteristics of security vulnerabilities specific to connected cars and derive checklists, but we had to narrow the scope due to the mentioned risk issues that may occur in vehicles. If future research is conducted in collaboration with vehicle manufacturers and an environment is created where tests can be conducted on vehicles or manufacturer servers, we expect that this aspect can be strengthened to identify the characteristics of security vulnerabilities unique to connected cars, add them to the checklist, and conduct actual vulnerability analysis to derive more meaningful results.

Acknowledgement

This research was funded by a 2021 research Grant from Sangmyung University.

References

- [1] S. Lenfle and C. Midler, "The launch of innovative product-related services: lessons from automotive telematics," *Research Policy*, vol. 38, no. 1, pp. 156-169, 2009. <https://doi.org/10.1016/j.respol.2008.10.020>
- [2] A. Akram and M. Akesson, "Value network transformation by digital service innovation in the vehicle industry," in *Proceedings of the 15th Pacific Asia Conference on Information Systems (PACIS)*, Brisbane, Australia, 2011.
- [3] HIS iSuppli Inc., "Embedded Telematics in the Automotive Industry," 2011 [Online]. Available: http://gallery.mailchimp.com/e68b454409061ef6bb1540e01/files/Embedded_Telematics_in_the_Automotive_Industry_sw_iS.pdf.
- [4] J. Ohlsson, P. Handel, S. Han, and R. Welch, "Process innovation with disruptive technology in auto insurance: lessons learned from a smartphone-based insurance telematics initiative," in *BPM - Driving Innovation in a Digital World*. Cham, Switzerland: Springer, 2015, pp. 85-101. https://doi.org/10.1007/978-3-319-14430-6_7
- [5] J. E. Park and M. Y. Yoon, "Hyper-connected society and future services," *Information & Communications Magazine*, vol. 31, no. 4, pp 3-9, 2014.
- [6] S. Vimalkumar, P. Hemalatha, and J. Kalaivani, "A review on smart IOT car for accident prevention," *Asian Journal of Applied Science and Technology*, vol. 2, no. 1, pp. 287-292, 2018.

- [7] Ernest & Young LLP, “The quest for Telematics 4.0,” 2013 [Online]. Available: <https://ey-france.relayto.com/e/the-quest-for-telematics-4-0-cbfjemm/QD7KnZgk1>.
- [8] S. G. Kim, “Rapid market expectations for connected cars under IoT/M2M technology environment,” *KISTI Market Report*, vol. 4, no. 2, pp. 3-6, 2014.
- [9] T. UcedaVelez, “Real world threat modeling using the pasta methodology,” in *Proceedings of the OWASP AppSec Research Conference*, Athens, Greece, 2012.
- [10] S. R. Do, “Trends in cybersecurity standards and threat analysis techniques,” *Weekly Tech Trends*, vol. 2019, no. 1918, pp. 2-15, 2019.
- [11] A. Shostack, *Threat Modeling: Designing for Security*. Indianapolis, IN: John Wiley & Sons, 2014 (Transl.: in H. Yang, editor, *Threat Modeling*. Seoul, Korea: Acorn Publishing Co., 2016).
- [12] Institute of Information & communications Technology Planning & Evaluation, “Intelligent vehicle security threats and countermeasures report,” 2017 [Online]. Available: <https://www.itfind.or.kr/report/analysis/read.do?selectedId=02-004-171208-000018>.
- [13] A. D. Kumar, K. N. R. Chebrolu, R. Vinayakumar, and K. P. Soman, “A brief survey on autonomous vehicle possible attacks, exploits and vulnerabilities,” 2018 [Online]. Available: <https://doi.org/10.48550/arXiv.1810.04144>.
- [14] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, “Security and privacy vulnerabilities of In-Car wireless networks: a tire pressure monitoring system case study,” in *Proceedings of 19th USENIX Security Symposium (USENIX Security 10)*, Washington, DC, USA, 2010. <https://dl.acm.org/doi/10.5555/1929820.1929848>
- [15] J. Petit, M. Feiri, and F. Kargl, “Revisiting attacker model for smart vehicles,” in *Proceedings of 2014 IEEE 6th International Symposium on Wireless Vehicular Communications (WiVeC)*, Vancouver, Canada, 2014, pp. 1-5. <https://doi.org/10.1109/WIVEC.2014.6953258>
- [16] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, “Remote attacks on automated vehicles sensors: experiments on camera and LiDAR,” in *Proceedings of the Black Hat Europe*, Amsterdam, The Netherlands, 2015.
- [17] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, et al., “Experimental security analysis of a modern automobile,” in *Proceedings of 2010 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2010, pp. 447-462. <https://doi.org/10.1109/SP.2010.34>



Jin Kim <https://orcid.org/0000-0002-9632-5672>

He received B.S. degree in metallurgical engineering and material science from Hongik University in 2000, M.S. degree in information media strategies from Yonsei University in 2014, and Ph.D. degree in business administration from Sangmyung University in 2022. He is currently a professor in the Big Data Convergence Major, Sangmyung University, Seoul, Korea. His research interests include Big data and cyber security.



Jinho Yoo <https://orcid.org/0000-0003-4359-8009>

He is a professor at Sangmyung University. He received his B.S. degree in Mathematics and M.S. in Statistics and Ph.D. degrees in Information Management and Security at Korea University. Prior to joining Sangmyung University, he worked as a director of the Korea Internet and Security Agency, as a managing consultant of CRM and data mining at IBM, and as a researcher of R&D planning at the Electronics and Telecommunications Research Institute. His research interests include issues related to information security & privacy, big data analytics, blockchain and data mining.