IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 27, 2020, accepted June 9, 2020, date of publication June 24, 2020, date of current version July 9, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3004661

Practical Vulnerability-Information-Sharing Architecture for Automotive Security-Risk Analysis

YOUSIK LEE[1], SAMUEL WOO[2], YUNKEUN SONG[1], JUNGHO LEE[3], AND DONG HOON LEE[4], (Member, IEEE)

[1]ESCRYPT GmbH, Gyeonggi 13488, South Korea
[2]Department of Software Science, Dankook University, Gyeonggi 16891, South Korea
[3]Korea Information Certificate Authority Inc., Gyeonggi 13488, South Korea
[4]Graduate School of Information Security, Korea University, Seoul 02841, South Korea

Corresponding author: Dong Hoon Lee (donghlee@korea.ac.kr)

This work was supported by the Institute for Information and Communications Technology Promotion (IITP) funded by the Korea Government (MSIT) (Developing Technologies to Predict, Detect, Respond, and Automatically Diagnose Security Threats to Automotive Ethernet-Based Vehicle) under Grant 2018-0-00312.

ABSTRACT Emerging trends that are shaping the future of the automotive industry include electrification, autonomous driving, sharing, and connectivity, and these trends keep changing annually. Thus, the automotive industry is shifting from mechanical devices to electronic control devices, and is not moving to Internet of Things devices connected to 5G networks. Owing to the convergence of automobile-information and communication technology (ICT), the safety and convenience features of automobiles have improved significantly. However, cyberattacks that occur in the existing ICT environment and can occur in the upcoming 5G network are being replicated in the automobile environment. In a hyper-connected society where 5G networks are commercially available, automotive security is extremely important, as vehicles become the center of vehicle to everything (V2X) communication connected to everything around them. Designing, developing, and deploying information security techniques for vehicles require a systematic security-risk-assessment and management process throughout the vehicle's lifecycle. To do this, a security risk analysis (SRA) must be performed, which requires an analysis of cyber threats on automotive vehicles. In this study, we introduce a cyber kill chain-based cyberattack analysis method to create a formal vulnerability-analysis system. We can also analyze car-hacking studies that were conducted on real cars to identify the characteristics of the attack stages of existing car-hacking techniques and propose the minimum but essential measures for defense. Finally, we propose an automotive common-vulnerabilities-and-exposure system to manage and share evolving vehicle-related cyberattacks, threats, and vulnerabilities.

INDEX TERMS Automotive cybersecurity, automotive CVE, cyber kill chain, information sharing, security risk analysis.

I. INTRODUCTION

Modern vehicles now incorporate a variety of electronic controls that can enable effective adherence to emission regulations while providing a comfortable and safe driving environment to the users [1]. This convergence of automotive and ICT has become a new paradigm for the development of next-generation automobiles. Based on an analysis of the latest automobile industry trends, Pricewaterhouse-Coopers (PwC), a global consulting firm, coined a term outlining the future direction of automobile development as "EASCY" [2], which stands for *Electrified, Autonomous, Shared, Connected, and updated Yearly*. The tenets of EASCY suggest that automobiles have now evolved into Internet of Things (IoT) devices that are always connected to external networks such as 5G.

PwC compiled a report based on its analysis, which predicts that by 2030, 51 % of vehicles will be equipped with

The associate editor coordinating the review of this manuscript and approving it for publication was Ilsun You.

autonomous driving capabilities in some form. An organic combination of connected technology and sensor-based autonomous driving technology is essential for automated driving systems to understand the environment around the vehicle and adhere to the norms for autonomous driving. The US Department of Transportation (US DoT) calls this category of automobiles connected and automated vehicles (CAVs). However, with the development of CAVs aided by the convergence of automotive and communications technologies such as 5G, the automotive ecosystem is now being exposed to security threats that exist in the ICT environment [3]. However, many automotive manufacturers still see cars as independent machines operating in closed environments and have not applied the same level of security technology to cars as compared to actual ICT environments.

Over the past decade, the automotive security community, through vulnerability analysis and hacking studies using actual automotive vehicles [4], has proved that automobiles are also susceptible to cyber-attacks. In one particular instance in 2015, a large-scale recall operation had to be performed based on the results of a car hacking study conducted by Charlie Miller *et al.* The recall resulted in huge economic losses for the car manufacturer [5]. After the incident, not only automotive manufacturers but also governments and auto-related organizations have begun publishing guidelines, laws, and regulations for auto cyber defenses to ensure passenger safety and minimize economic losses. In recent years, the United Nations Economic Commission for Europe (UNECE) has formulated regulations to include cybersecurity in the approval process of vehicle types. The regulator needs to evaluate the effectiveness of the cybersecurity management system installed by car manufacturers. Certification schemes for these systems have also been discussed at length [6].

A key requirement for regulations and certifications related to automotive cyber-security is the implementation of a systematic security risk assessment and management process during the vehicle's lifecycle, which includes the development, production, and post-production control phases [7]. The security risk assessment and management process for vehicles requires monitoring and evaluating threats throughout the lifecycle and sharing the results of the assessments to respond appropriately to evolving security threats. It is also important to identify assets and risks based on these collected, evaluated, and shared threats, and to accurately analyze and assess the security risks that can occur in the vehicle. This series of steps can be accomplished through security risk analysis (SRA). [21]

FIGURE 1. Security-risk-analysis process [8].

As shown in Figure 1, threat modeling is the essential step of SRA. Cyber threats will continue to increase and evolve as long as the threat agent exist. Therefore, it is very important to identify new and evolving cyber threats and vulnerabilities to vehicles. In this sense, cyber security monitoring processes and vulnerability/threats sharing platforms are effective to update information on new and evolving cyber threats and vulnerabilities. In this study, we analyze the characteristics of the car hacking techniques that have occurred from 02010. Additionally, a cyber kill chain-based cyberattack analysis method is introduced to prepare formal vulnerability analysis and hacking technology analysis system. Through this study:

1) We analyzed 11 major hacking studies based on the cyber kill chain methodology.
2) Based on the results of the cyber kill chain analysis, we identified common security measures that should be considered in modern vehicles, and suggested a new course of action matrix for the vehicle environment.
3) We propose an automotive common vulnerabilities and exposure (CVE) system that enables car security researchers and engineers to share technical information on vulnerability analysis and hacking cases performed on automobiles. We have created a beta version of our website where we can share information about our automotive CVE system. (Site address: https://automotive-cve.com)

The goal of this study is to analyze attack cases from the attacker's perspective and provide common countermeasures based on the cyber kill chain methodology. The scope of this study does not include the quantification of risk.

This paper is organized as follows: Section 2 provides background information about the necessity of automobile security and the methodology used to analyze hacking cases. Section 3 provides a detailed analysis of the three hacking cases and a summary of the analysis results. Section 4 describes the automotive CVE, and Section 5 provides the conclusion.

II. BACKGROUND

A. SECURITY RISK ANALYSIS

SRA is a methodology used to estimate the risk and possible damage to assets. It determines the level of risks based on the attack potential of threats and the potential damage if the assets are compromised. The security of the targeted assets is assured by appropriate risk management, which is a result of SRA. The SRA consists of five processes shown in Figure 1 [8].

Threat modeling during the SRA process identifies potential attack vectors that could intentionally interfere with specific vehicle functions. In this case, the attack tree shown in Figure 2 is used to analyze the methods that an attacker can employ to interfere with the target. When constructing the attack tree, the threat catalog is utilized and the attack methods are identified. The threat catalog is a list of known threats. As long as threat sources exist, threats and vulnerabilities continue to increase; thus, one must review

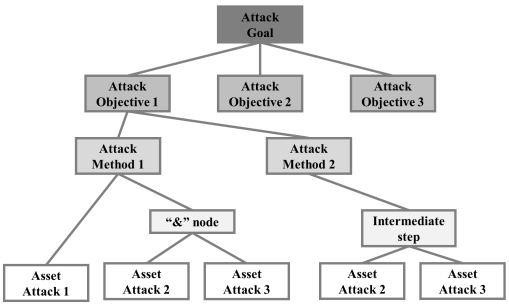


FIGURE 2. General structure of attack tree [9].

new threats and update the information in the threat catalog. Continuous monitoring processes and information sharing systems should be established to identify emerging cyber threats and vulnerabilities.

B. CYBER KILL CHAIN

Cyber kill chain refers to the process of analyzing cyber-attacks to identify threats to the organization at each stage of the attack, crushing and mitigating the attacker's purpose, and planning and implementing measures to secure the organization system [10]. The cyber kill chain is composed of seven levels as shown in Figure 3. The seven levels are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. The description of each stage of the cyber kill chain is provided in Table 1.

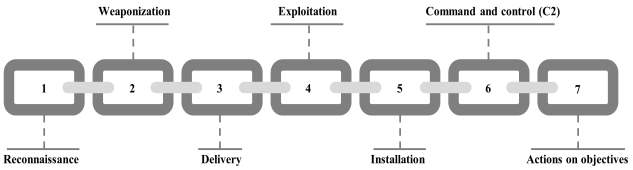


FIGURE 3. Seven steps of the cyber kill chain [10].

III. ANALYSIS OF AUTOMOTIVE CYBER ATTACK BASED ON CYBER KILL CHAIN

Since the Washington University researchers conducted the vulnerability assessment study on cars in 2010, various types of vulnerability analysis and hacking studies have been published on vehicle electronic control systems. In this section, we analyze automotive hacking techniques reported in the academic and automotive industries. Cyber kill chain analysis was used to analyze and organize the attack process and attack characteristics of each hacking technique in a consistent manner. The representative studies based on the cyber kill chain are listed in Table 2.

To explain the cyber kill chain-based threat analysis method, a representative study for each attack type was selected from the studies listed in Table 2 and detailed analysis was performed. For the remaining studies, only the analysis results analyzed by the cyber kill chain are listed.

TABLE 1. Cyber kill chain [10].

Cyber kill chain	Description
Reconnaissance	Information gathering steps for the target and method of attack
Weaponization	Steps to create malware or attack tools to be used in an attack
Delivery	Steps to find a way to deliver malware or attack tools to targets
Exploitation	Malware or an attack tool is delivered to an attack target
Installation	The stage in which the malware or attack tool is installed and run on the victim, and additional malware is downloaded
Command and Control	Malware or an attack tool is associated with a command control server, leaving control of the attack target to the attacker
Actions on Objectives	State of malicious activity such as data leakage or destruction

TABLE 2. Automotive cyberattack cases.

No	Year	Title
1	2019	Enhanced Android App-Repackaging Attack on In-Vehicle Network [11]
2	2017	WANNADRIVE? Feasible Attack Paths and Effective Protection Against Ransomware in Modern Vehicles [12]
3	2017	Free-Fall: Hacking Tesla from Wireless to CAN Bus [13]
4	2017	Vulnerabilities of Android OS-Based Telematics System [14]
5	2015	Remote Exploitation of an Unaltered Passenger Vehicle [5]
6	2014	A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN [15]
7	2013	Adventures in Automotive Networks and Control Units [16]
8	2011	Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars [17]
9	2011	Comprehensive Experimental Analyses of Automotive Attack Surfaces [18]
10	2010	Experimental Security Analysis of a Modern Automobile [19]
11	2010	Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study [20]

A. AN EXAMPLE USE CASE OF AUTOMOTIVE CYBER KILL CHAIN

To study the use cases, we selected three representative studies from the list in Table 2 and analyzed the attack techniques in detail and categorized those as cyber kill chain.

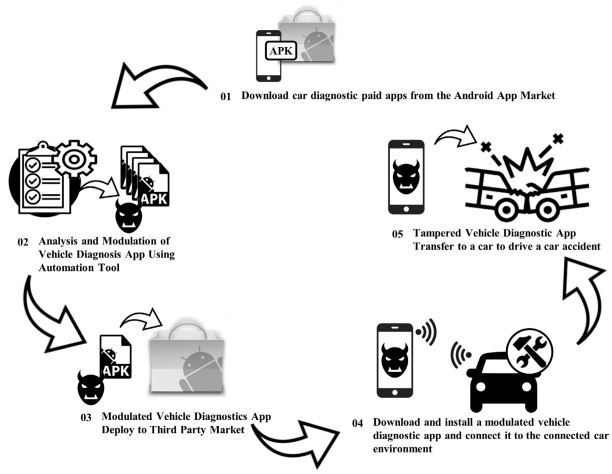


FIGURE 4. Attack model of attack case no. 1 [11].

1) USE CASE 1: ENHANCED ANDROID APP-REPACKAGING ATTACK ON IN-VEHICLE NETWORK [11]

Lee *et al.* defined an attack model using the ELM327 command protocol and a vehicle management application to create a connected automotive environment and conducted hacking experiments on actual vehicles. Figure 4 shows the overall flow of this experiment. Lee *et al.* planned the cyber-attack in three steps.

The first step was the environmental analysis of the ELM327 module and the fleet management app that constitute the connected car environment. They analyzed the communication process and the AT (Attention) command of the ELM327 through an open document and succeeded in forcibly controlling the vehicle using the AT command. The vulnerability analysis was performed based on the operating principle of the vehicle management app distributed through the Android market and the smali code obtained by reverse-engineering the app. This phase corresponds to the cyber reconnaissance phase.

The second step involved tampering with the android repackaging of the app distributed on the Android market. They analyzed the characteristics of the ELM327 and fleet management apps were used to create a connected car environment and then transformed the distributed commercial apps into malicious apps. They modulated the AT Command and the vehicle management app analyzed in the first step and were then injected into the vehicle. This stage corresponds to the weaponization and dissemination of the cyber kill chain.

The third stage is an attack experiment using an actual automotive vehicle. Lee *et al.* conducted a forced maneuver control experiment assuming that a modified fleet management app was redistributed through the black market and on the android marketplace and installed it on the victim's smartphone. At this stage, the disseminated app distribution and victim's download behavior assumed by Lee *et al.* correspond to the dissemination and exploitation of the cyber kill chain, respectively.

The victim installs a modified fleet management app on his smartphone and creates a connected car environment using ELM327. The modulated fleet management app transmits a compulsory control message to the vehicle base on the specific conditions of the vehicle (revolutions per minute (RPM), speed, app driving, etc.). The vehicle received the forced control message in an abnormal state and the attack simulation is successful. The final stage of the attack experiment conducted by Lee *et al.* was the installation, command and control, and achievement of the cyber kill chain. The analysis of the cyber-attacks performed by Lee *et al.* in terms of the cyber kill chain is listed in Table 3.

TABLE 3. Cyber kill chain analysis results of attack case no. 1.

Cyber kill chain	Description
Reconnaissance	• In-vehicle CAN message analysis of vehicle • Environmental analysis such as ELM327 communication process and AT command to create a connected car environment • Vehicle management app and environment analysis distributed on Android market
Weaponization	• Acquire AT command to control the vehicle using ELM327 • Identify the vulnerabilities of the vehicle management app deployed in the Android market • Modulate fleet management app using Android repackaging • Create an installable APK file using self-signing
Delivery	• Deploy to Android Market • Deploy to Android black market (3rd party market), which distributes paid apps for free
Exploitation	• Victim downloads modified fleet management apps through the Android market or Android black market
Installation	• Install the downloaded app on your smartphone • ELM327 mounted on the vehicle to create a connected car environment
Command and Control	• Forced control command transfer in specific condition (RPM, speed, App driving) set in the modified vehicle management app
Actions on objectives	• Cause traffic accident of vehicle by sending vehicle forced control command (the simulation achieved its purpose)

2) USE CASE 2: WANNADRIVE? FEASIBLE ATTACK PATHS AND EFFECTIVE PROTECTION AGAINST RANSOMWARE IN MODERN VEHICLES [12]

Wolf *et al.* demonstrated how a ransomware attack can be performed on a vehicle using a real device and suggested effective defense techniques. Ransomware is known as the most successful and profitable attack technique in traditional IT environments. In the automotive industry, assuming that 10 % of the 250 million connected cars in 2020 are infected with ransomware, protection for 20 % of them at an average cost of $200 can potentially create a market of over US $1 billion. Therefore, effective measures are needed in the automobile industry for protection against ransomware. Ransomware has no reconnaissance phase for a particular vehicle because many unspecified vehicles are targeted. At stage,

ransomware can be produced inexpensively and easily using Ransomware-as-a-service (RaaS) such as TOX or STAMP, which are ransomware toolkits.

In the delivery step, ransomware can be deployed using a botnet such as TOR-based MIRAI with 400,000 client bots at a cost of $1,000 per week. The distributed ransomware can be distributed to a vehicle indirectly by infecting a web service or a host PC to which a head unit or infotainment system of a vehicle is connected, or distributed to a vehicle through a USB, an on-board diagnostics (OBD) device, or a diagnostic device. The delivered ransomware can be installed by exploiting a vulnerability in the automotive software. The installed ransomware locks the main components of the car so that it cannot be used through encryption at the command and control stage. Subsequently, the victim is asked for anonymized rewards such as Bitcoins, and when the victim sends the required Bitcoins, the unlocked components can be released and used again. The analysis of cyber-attacks performed by Wolf *et al.* in terms of the cyber kill chain is listed in Table 4.

TABLE 4. Cyber kill chain analysis results of attack case no. 2.

Cyber kill chain	Description
Reconnaissance	• Vulnerability analysis of IoT devices installed in vehicles
Weaponization	• RaaS such as TOX and STAMP, which includes functions such as a control server (botmaster) and payment system (Bitcoin)
Delivery	• Distribution of Ransomware through TOR-based botnets such as MIRAI : MIRAI offers 400,000 botnet clients at a cost of $ 1,000 per week : The botnet does not connect directly to the vehicle but infects and misuses the vehicle's systems through various attack surfaces.
Exploitation	• Ransomware delivery through various attack surfaces of the vehicle (infotainment system, head unit, USB port, OBD, CD / DVD)
Installation	• Run ransomware automatically when the vehicle starts
Command and Control	• Locks key components that cannot be easily restored : ECU key features, critical data in the vehicle, cryptographic credential
Actions on objectives	• Victim's payment (the attacker's financial gain)

3) USE CASE 3: A PRACTICAL WIRELESS ATTACK ON THE CONNECTED CAR AND SECURITY PROTOCOL FOR IN-VEHICLE CAN [15]

Woo *et al.* defined an attack model using a smartphone application in a connected car environment and conducted a cyber-attack experiment using a real car. Figure 6 shows the overall flow of this experiment.

Three steps constituted the cyber-attack performed by Woo *et al.* The first step is to acquire a controller area network (CAN) packet that can force control of the target vehicle. After monitoring the network traffic generated from

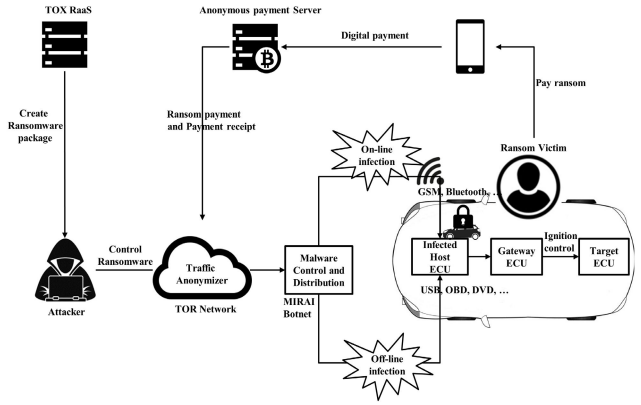


FIGURE 5. Attack model of attack case no. 2 [12].

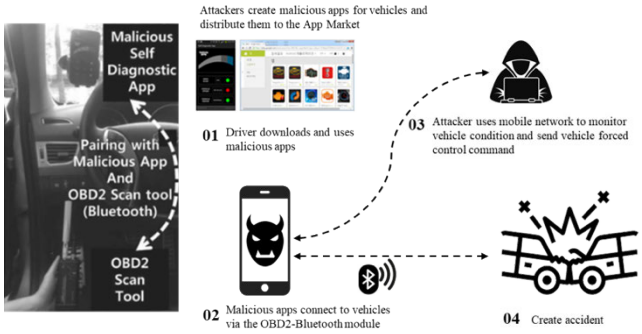


FIGURE 6. Attacker model of attack case no.6. [15].

the target vehicle's in-vehicle CAN, the attacker obtained the CAN packet to gain control of the vehicle through full packet inspection and fuzzing test. They also connected the car maintenance equipment to the target vehicle and analyzed the communication between the car and maintenance equipment to obtain a CAN packet that can be forcibly controlled. The first phase corresponds to the reconnaissance phase of the cyber kill chain.

The second step is to build a malicious app. After analyzing the characteristics of smartphone apps used in the connected car environment, they created malicious smartphone apps. The malicious smartphone app injects the forced control packet analyzed in step 1 into the target vehicle. The second phase corresponds to the reconnaissance and weaponization step of the cyber kill chain.

The last step is to experiment with actual cars. Woo et al conducted a cyber-attack experiment assuming that a malicious smartphone app was distributed through the App Market and installed on the victim's smartphone. Malicious app distribution and victim's download behavior assumed by Woo *et al.* correspond to the distribution and abuse of the cyber kill chain. The victim installs a malicious app on his smartphone and then connects the car to the malicious smartphone app using the CAN to Bluetooth module. The malicious smartphone app installed on the victim's smartphone communicates with the attack server using the mobile communication network. The attacker analyzes the optimal attack time based on the vehicle status information received from the

malicious app and sends the attack command. The malicious smartphone app that receives the attack command injects a forced control packet into the in-vehicle CAN through the CAN to Bluetooth module. The electronic control device of the vehicle in which the forced control packet is injected falls into an abnormal state (engine stop, rapid acceleration, and so on.).

The final stages of the attack experiment conducted by Woo *et al.* were the installation, command, and control of cyber kill chains and the achievement of goals. The analysis of cyberattacks performed by Woo et al in terms of the cyber kill chain is listed in Table 5.

TABLE 5. Cyber kill chain analysis results of attack case no. 6.

Cyber kill chain	Description
Reconnaissance	• In-Vehicle CAN traffic analysis of target vehicle • Smartphone app analysis in the connected car environment
Weaponization	• Develop malicious smartphone apps (equipped function for receiving commands from attack server • Create built-in CAN packet to force control the target vehicle) • Malicious smartphone apps have normal self-diagnosis
Delivery	• Upload malicious smartphone apps disguised as apps for self-diagnosis to the App market
Exploitation	• Drivers download malicious smartphone apps
Installation	• The driver installs the downloaded malicious smartphone app on his smartphone • Use the app by wirelessly connecting the car and the malicious smartphone app using the CAN to Bluetooth module
Command and Control	• Receive commands from the attack server
Actions on objectives	• When the attack command is received, a packet that can forcibly control the target vehicle is injected into the in-vehicle CAN through the can to Bluetooth module, causing a traffic accident (achieving the purpose)

B. ANALYSIS RESULT OF AUTOMOTIVE CYBER KILL CHAIN

This section describes the cyber kill chain analysis results for the hacking cases from the studies listed in Table 2.

1) FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS [13]

See Table 6.

2) VULNERABILITIES OF ANDROID OS-BASED TELEMATICS SYSTEM [14]

See Table 7.

TABLE 6. Cyber kill chain analysis results of attack case no. 3.

Cyber kill chain	Description
Reconnaissance	• Analysis of access point and password vulnerability of free Wi-Fi AP provided by Tesla charging station : There is a function to automatically access the free AP in the charging station provided by Tesla : AP's SSID (name) and password are almost the same and can be easily deduced • Analysis of security vulnerabilities of Tesla's embedded infotainment device and embedded browser : Linux-based infotainment device automatically refreshes open web pages when accessing AP : Vulnerability that can execute arbitrary code on an infotainment device when refreshing in a web browser (CVE-2011-3928) can be exploited • Analysis of firmware change shows the possibility of controllers connecting infotainment equipment and in-vehicle network : Verification of the firmware installation file when updating the controller firmware through OTA is done by the file name
Weaponization	• Malicious AP production, attack web page production • Firmware forcing controller
Delivery	• Malicious AP Installation
Exploitation	• Attack web pages • Firmware download to force controller
Installation	• Install firmware to force controller
Command and Control	• Forced control of the vehicle through the controller after the controller's firmware is installed
Actions on objectives	• Complete vehicle forced control success

3) REMOTE EXPLOITATION OF AN UNALTERED PASSENGER VEHICLE [5]

In this hacking case, the attack tool created in the weaponization step is installed on the identified attack target through the reconnaissance step. As a result, the process of delivery, exploitation, and installation is integrated into one process.

The attack process and characteristics in this hacking case is very similar to the wireless attack model that the University of Washington conducted in 2011; hence, the cyber kill chain analysis of the University of Washington case is omitted.

4) ADVENTURES IN AUTOMOTIVE NETWORKS AND CONTROL UNITS [16]

The attack process and characteristics of this hacking case and the University of Washington research case conducted in 2010 are similar. Hence, the cyber kill chain analysis of the University of Washington case is omitted.

TABLE 7. Cyber kill chain analysis results of attack case no. 4.

Cyber kill chain	Description
Reconnaissance	• Gain firmware sample • Analyze automobile forced control message through binary file analysis
Weaponization	• Create attack code insertion for forced car control • Create malicious firmware
Delivery	• Deliver through P2P site, community site, torrent, etc.
Exploitation	• Victims (car owners) download malicious firmware via the Internet, community, etc.
Installation	• Victims (car owners) use the recovery mode of the telematics system to install malicious firmware in their cars
Command and Control	• The attacker sends an SMS for forced control (remote door unlocking, location tracking) from the mobile phone number of the telematics device with malicious OTA firmware installed
Actions on objectives	• The attacker forces control of the car door and receives location information

TABLE 8. Cyber kill chain analysis results of attack case no. 5.

Cyber kill chain	Description
Reconnaissance	In this attack case, the reconnaissance process is divided into primary reconnaissance and secondary reconnaissance. • Primary reconnaissance : Wi-Fi password cracking for wireless connection to Uconnect system : Uconnect system port scanning : Check if the authentication option of D-BUS protocol is used : Obtain root authority of the Uconnect system and analyze service provided : Identify the execute method to use for the attack : Firmware collection and vulnerability identification • Secondary reconnaissance : Scanning targets for attack tool installation
Weaponization	• Create scripts for compulsory vehicle control • Create malicious firmware
Delivery Exploitation Installation	• Identify target vehicles by scanning port 6667 on specific IP bands (21.0.0.0/8, 25.0.0.0/8) using the US Sprint network • Flash malicious firmware on the Uconnect system of the target vehicle
Command and Control	• Force control command sent to victim vehicle with malicious firmware
Actions on objectives	• Forced vehicle control (steering, breaks, engine, turn signal, locks, RPMs, HVAC, radio volume, etc.)

5) RELAY ATTACKS ON PASSIVE KEYLESS ENTRY AND START SYSTEMS IN MODERN CARS [17]

In this hacking case, an attacker directly installs an attack tool created in the weaponization step near the target to perform the attack. As a result, the steps of delivery, exploitation, and installation are integrated into one process.

TABLE 9. Cyber kill chain analysis results of attack case no. 7.

Cyber kill chain	Description
Reconnaissance	• CAN bus structure and CAN message analysis in In-Vehicle network • Firmware Extraction and Reversing • Reversing the Firmware Update Software (Calibration Update Wizard, CUW) • Firmware re-flashing process analysis
Weaponization	• Generate vehicle forced control CAN message • Create malicious firmware
Delivery Exploitation Installation	• Malicious firmware flash via CAN bus
Command and Control	• The car forced control CAN message sent to the in-vehicle network
Actions on objectives	• Forced vehicle control (steering, braking, acceleration, engine, speedometer, odometer, horn, doors, seat belt motor, HAVC, etc.)

TABLE 10. Cyber kill chain analysis results of attack case no. 8

Cyber kill chain	Description
Reconnaissance	• Identify the characteristics of PKES : Vehicle function operation method according to the key position (remote, inside, outside)
Weaponization	• Create equipment for amplifying and relaying wireless signals
Delivery Exploitation Installation	• The attacker installs the attack tool created during the weaponization step in two locations. : Installation location 1: Car, installed near the PKES : Installation Location 2: Smart Key Proximity Point of Target Vehicle
Command and Control	• The attacker starts his equipment to amplify communication data between PKCS and Key and relay
Actions on objectives	• Unlock the car door and start the engine

6) SECURITY AND PRIVACY VULNERABILITIES OF IN-CAR WIRELESS NETWORKS: A TIRE PRESSURE MONITORING SYSTEM CASE STUDY [20]

In this hacking case, an attacker directly installs an attack tool created in the weaponization step near the target to perform the attack. Because of this, the steps of delivery, exploitation, and installation are integrated into one.

C. COUNTERMEASURES BASED ON A COURSE OF ACTION MATRIX

If cyberattacks on vehicles can be analyzed using the cyber kill chain methodology, defenders can plan and design

TABLE 11. Cyber kill chain analysis results of attack case no. 11.

Cyber kill chain	Description
Reconnaissance	• TPMS system structure analysis, TPMS communication protocol analysis, TPMS wireless communication vulnerability analysis, TPMS packet analysis
Weaponization	• Create a TPMS signal activation device (TPMS packet analysis) • Create TPMS packet-based vehicle analysis tool (vehicle tracking, event triggering) • Create TPMS packet tampering-transmitter fabrication (packet tampering, DoS attack)
Delivery Exploitation Installation	• Install attack tools created during the weaponization step at major attack points. • Perform signal activation attacks on all vehicles • Repeat until the target vehicle appears
Command and Control	• Attacking when target vehicle detection is activated Attack 1: Vehicle tracking, Attack 2: Event triggering, Attack 3: Packet tampering, DoS
Actions on objectives	• Achieve vehicle location tracking, • TPMS system malfunction, TPMS sensor battery DoS

countermeasures using a course of action matrix. A course of action matrix uses the actions of detect, deny, disrupt, degrade, deceive, and destroy. Figure 8 shows the course of action matrix for typical advanced persistent threat attacks [10].

However, automotive environments differ from traditional information security environments. Because we analyze important attack cases, we can map between effective countermeasures to respective attack cases and each steps of perspective of cyber kill chain. Figure 7 provides capable countermeasures for every attack cases we analyzed. The list of countermeasures in this table is not exhaustive, and it is not be necessary to apply all countermeasures listed

Phase	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control	Actions on objectives
Case 1	Obfuscation	App signing	Android market policy		Signature verification	Whitelist based access control, Firewall	
Case 2							
Case 3	Obfuscation		Endpoint malware protection, Network segmentation	IDS	Secure flash, Security access	Firewall, IDS	
Case 4	Obfuscation	App signing			Signature verification, Access control	Authentication, App signing	
Case 5	Firewall, Obfuscation		Authentication, Firewall			Authentication	Authentication
Case 6							
Case 7	Obfuscation, AUTOSAR SecOC						
Case 8					Reduced frequency range	Distance bound protocol	
Case 11	Encryption					Authentication	

FIGURE 7. Countermeasures for the attack cases.

Now, we propose a new course of action matrix for vehicles, especially in-vehicle networks based on the mapping table. Because the communication between vehicles and external components of a vehicle such as infra systems, servers, and other vehicles is similar to a traditional information security environment, we focus on the vehicle itself.

Figure 10 shows the new course of action matrix for vehicles.

In general, a vehicle consists of many components like electric control units, and vehicle manufacturers are provided these components from several suppliers. To ensure the security of vehicles, all providers as well as vehicle manufacturers must be able to implement security measures.

This is the reason why supply chain security and a secure platform are important. A secure platform refers to the platform where secure boot, secure flash, and secure access are applied. The hacking cases we analyzed have actions at an installation phase, i.e. a secure platform can prevent almost all hacking attempts.

Thus, all vehicle manufacturers must request suppliers to implement a secure platform and the suppliers must implement it because it is one of the basic and essential measures to effectively protect vehicles from cyber-attacks.

IV. AUTOMOTIVE-CVE

In the traditional cyber-security field, there are vulnerability information sharing systems such as CVE, national vulnerability database (NVD), and common weakness enumeration (CWE).

CVEs are operated to standardize the detection of security vulnerabilities [22]. This enables security officers to find and use technical information about specific threats. More than 133,000 vulnerabilities are currently registered [23].

However, CVEs mainly share vulnerabilities of general IT environments, especially network-related IT environments, and finding a weakness in the automotive sector requires lots of effort. It is difficult for automotive engineers to determine if the specific vulnerability is related to the automotive industry unless they are cybersecurity experts.

NVD was established to provide detailed information related to CVE's vulnerability list. NVD is a database operated by the National Institute of Standards and Technology (NIST) and provides a technical perspective on the respective vulnerability as well as a score of common vulnerability scoring systems (CVSS) and related CWE information. [24]

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall, ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
Command and Control	NIDS	Firewall, ACL	NIPS	Tarpit	DNS Redirect	
Actions on objectives	Audit log			Quality of Service	Honeypot	

FIGURE 8. Course of action matrix.

CWE is a list of common software and hardware security weakness to supports building secure software. 839 security weaknesses were registered as of April 2020. [25]

Automotive Information Sharing and Analysis Center (Auto-ISAC) is an organization for sharing automotive security vulnerabilities. Auto-ISAC was founded in August 2015 by car manufacturers. As of April 2019, 49 manufacturers and parts companies, including more than 30 global OEMs, have joined to exchange information such as hacks and vulnerabilities [26]. However, Auto-ISAC provides the information only to members, and because only vehicle manufacturers and parts companies can be members because of the size of their membership, researchers at small companies, individuals, or research institutes have limited access to the information.

In this study, an automotive CVE was developed to share car security-related vulnerabilities and attack cases with anyone interested and to overcome the limitations of CVE, NVD, CWE, and Auto-ISAC [27]. Two things are considered important in this study:

- Vulnerability list for automotive industry
- Openness to public

Automotive CVE shares vulnerabilities regarding the automotive industry that is easily accessible to automotive engineers who have limited security expertise.

	CVE	NVD	CWE	Auto-ISAC	A-CVE
Operating Org	MITRE	NIST	MITRE	Auto-ISAC	AEGIS
Operating Country	USA	USA	USA	USA	KOREA
Openness	Public	Public	Public	Closed	Public
Target	IT	IT	IT	Automotive	Automotive
Item	Vulnerability list	Detailed vulnerability information	Security weakness	Automotive related vulnerability	Automotive related vulnerability

FIGURE 9. Comparison of vulnerability sharing system.

Figure 9 shows the characteristics of the vulnerability sharing systems.

An automotive CVE analyzes and shares individual vulnerabilities from the following sources:

- Share request by voluntary participation
- Automotive-related information reported to CVE
- Continuous monitoring

An automotive CVE has been built, managed, and operated by AEGIS, an automotive cybersecurity research organization. AEGIS frequently analyzes car vulnerability information through CVE monitoring and automobile security research surveys and registers the results with the automotive CVE.

When registering, CVE sources and links are added. Voluntary registration requests by researchers or engineers may be provided in the following form.

- Threat ID
- Related manufacturer/providers
- Related vehicle name
- Problem type
- References

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance		Firewall, ACL[2]	MDT, Obfuscation, AUTOSAR SecOC[1]	Authenticated diagnostics		
Weaponization						
Delivery	Endpoint malware protection	SOTA[5], Network segmentation		Authenticated diagnostics		
Exploitation	IDS[4]	Patch	Secure storage	Security testing		
Installation	Secure boot, HSM (real time detection)	Secure flash		Security access		Roll back (SOTA[5]), Secure flash
Command and Control	IDS[4]	Firewall, ACL[2]	MTD[3]			
Actions on objectives	Audit log	Data encryption				

[1]: SecOC: Secure Onboard Communication
[2]: ACL: Access Control List
[3]: MTD: Moving Target Defense
[4]: IDS: Intrusion Detection System
[5]: SOTA: Secure Over-the-air-update

FIGURE 10. Course of action matrix for vehicles.

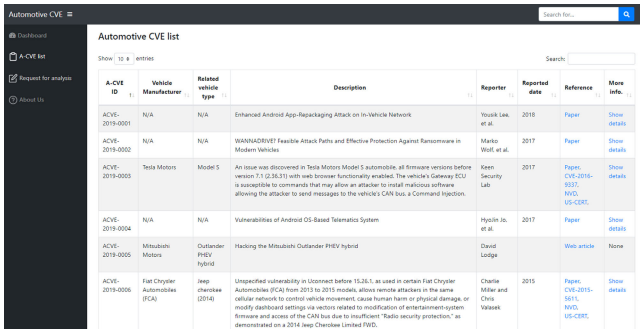


FIGURE 11. Automotive CVE website.

- Description
- Reporter
- Whether to open

V. CONCLUSION

To create a safe vehicle, the regulations stipulated by the UNECE should be followed, in addition to developing the security engineering process. It is well-known that the threat catalog, which is used to analyze threats, must be continuously updated for a successful SRA. However, the cyber kill chain methodology is adept at analyzing cyberattacks, threats, or vulnerabilities related to the automotive industry. In this study, we analyzed 13 major hacking cases based on the cyber kill chain methodology. Subsequently, we were able to learn more about attack stages with high frequency and derived common defense techniques. Additionally, an automotive CVE website was created to share the analyzed results, and operational methods and policies were established. It is assumed that more researchers and engineers will benefit from automotive CVE.

In the future, further research is required to activate the automotive CVE and to present each stage of defense techniques that can be utilized in the cyber kill chain.

REFERENCES

[1] A. Saad and U. Weinmann, "Automotive software engineering and concepts," in *Proc. GI Jahrestagung*, Frankfurt, Germany, vol. 34, 2003, pp. 318–319.

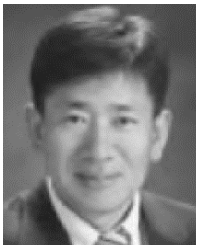
[2] F. Kuhnert, K. Sturmer, and A. Koste, "Five trends transforming the Automotive Industry, PwC," 2018.
[3] M. Wolf, A. Weimerskirch, and T. Wollinger, "State of the art: Embedding security in vehicles," *EURASIP J. Embedded Syst.*, vol. 2007, pp. 1–17, Dec. 2007.
[4] W. Wu, R. Li, G. Xie, J. An, Y. Bai, J. Zhou, and K. Li, "A survey of intrusion detection for in-vehicle networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 919–933, Mar. 2020.
[5] C. Miller, and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," Black Hat USA, 2015, p. 91.
[6] C. Schmittner and G. Macher, "Automotive cybersecurity standards—Relation and overview," in *Proc. SafeComp*, Turku, Finland, vol. 11699, 2019, pp. 153–165.
[7] G. Sabaliauskaite, J. Cui, L. S. Liew, and F. Zhou, "Integrated safety and cybersecurity risk analysis of cooperative intelligent transport systems," in *Proc. Joint 10th Int. Conf. Soft Comput. Intell. Syst. (SCIS), 19th Int. Symp. Adv. Intell. Syst. (ISIS)*, Dec. 2018, Art. no. 723728.
[8] M. Wolf and M. Scheibel, "A systematic approach to a qualified security risk analysis for vehicular IT systems," *Automot.-Saf. Secur.*, 2012.
[9] A. Ruddle, D. Ward, B. Weyl, S. Idrees, Y. Roudier, M. Friedewald, T. Leimbach, A. Fuchs, S. Gürgens, O. Henniger, and R. Rieke, "Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios," *EVITA Project*, 2009
[10] M. E. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Lead. Inf. Warfare Secur. Res.*, vol. 1, no. 1, p. 80, 2011.
[11] Y. Lee, S. Woo, J. Lee, Y. Song, H. Moon, and D. H. Lee, "Enhanced Android app-repackaging attack on in-vehicle network," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–13, Feb. 2019.
[12] M. Wolf, R. Lambert, T. Enderle, and A. D. Schmidt, "Wanna drive? Feasible attack paths and effective protection against ransomware in modern vehicles," in *Proc. Embedded Secur. Cars Conf. (ESCAR) Eur.*, 2017.
[13] S. Nie, L. Liu, and Y. Du, "Free-fall: Hacking tesla from wireless to can bus," in *Proc. BlackHat*, 2017, pp. 1–16.
[14] H. J. Jo, W. Choi, S. Y. Na, S. Woo, and D. H. Lee, "Vulnerabilities of Android OS-based telematics system," *Wireless Pers. Commun.*, vol. 92, no. 4, pp. 1511–1530, 2017.
[15] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993–1006, Apr. 2015.
[16] C. Miller, and C. Valasek, "Adventures in automotive networks and control units," *Def Con*, vol. 21, pp. 260–264, 2013.
[17] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *Proc. 18th Ann. NDSS*, 2011, pp. 1–24.
[18] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. USENIX Secur. Symp.*, San Francisco, CA, USA, 2011, p. 6.
[19] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, Oakland, CA, USA, 2010, pp. 447–462.
[20] I. Rouf, R. D. Miller, H. A. 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 *Proc. 19th USENIX Conf. Secur.*, Washington, DC, USA, 2010, pp. 1–16.
[21] D. Ward, I. Ibarra, and A. Ruddle, "Threat analysis and risk assessment in automotive cyber security," *SAE Int. J. Passenger Cars-Electron. Elect. Syst.*, vol. 6, no. 2, pp. 507–513, 2013.
[22] K. Seifried. *CVE-HOWTO*. Accessed: Dec. 2019. [Online]. Available: https://github.com/RedHatProductSecurity/CVE-HOWTO
[23] The MITRE Corporation. *Common Vulnerabilities and Exposures*. Accessed: Dec. 2019. [Online]. Available: https://cve.mitre.org/index.html
[24] National Institute of Standards and Technology. *National Vulnerability Database*. Accessed: Dec. 2019. [Online]. Available: https://nvd.nist.gov/general
[25] The MITRE Corporation. *Common Weakness Enumeration*. Accessed: Dec. 2019. [Online]. Available: https://cwe.mitre.org/
[26] *Auto-ISAC*. Accessed: Dec. 2019. [Online]. Available: https://www.automotiveisac.com/
[27] *Automotive-CVE*. Accessed: Dec. 2019. [Online]. Available: https://automotive-cve.com/acve_list

YOUSIK LEE is currently pursuing the Ph.D. degree in information security with Korea University. He has been in the cyber security industry for over 19 years, especially ten years in automotive security. He specializes in consulting, development and standardization for application security, PKI, cryptography, and automotive security. He is also a Security Consultant with ESCRYPT GmbH. His research interests include in-vehicle network security, V2X, security risk analysis, cybersecurity management systems (CSMSs), and evaluation methodologies for automotive security.

SAMUEL WOO received the Ph.D. degree in information security from Korea University, Seoul, South Korea, in 2016. He was a Senior Researcher with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, South Korea. He is currently an Assistant Professor with the Department of Software Science, Dankook University, Jukjeon, South Korea. His research interests include cryptographic protocols in authentication, security and privacy in vehicular networks, and controller area network security.

YUNKEUN SONG received the master's degree in information and communication engineering from Ajou University, Seoul, South Korea, in 2019. He is currently a Security Consultant with ESCRYPT GmbH, in 2017. His research interests include automotive security, cooperative-intelligent transport systems, and risk analysis methodologies.

JUNGHO LEE received the master's degree in information security from Korea University, Seoul, South Korea, in 2019. He joined the Korea Information Certificate Authority Inc., (KICA), in 2016. His research interests include V2X security, public key infrastructure (PKI), and vehicular security.



DONG HOON LEE (Member, IEEE) received the B.S. degree from the Department of Economics, Korea University, Seoul, South Korea, in 1985, and the M.S. and Ph.D. degrees in computer science from The University of Oklahoma, Norman, OK, USA, in 1988 and 1992, respectively. Since 1993, he has been with the Faculty of Computer Science and Information Security, Korea University. He is currently a Professor and the Director of the Graduate School of Information Security, Korea University. His research interests include cryptographic protocol, applied cryptography, functional encryption, software protection, mobile security, vehicle security, and ubiquitous sensor network (USN) security.