http://dx.doi.org/10.15207/JKCS.2015.6.5.033

Threat Issues of Intelligent Transport System in the V2X Convergence Service Envrionment

Jin-Keun Hong*
[1]Division of Information Communication, Baekseok University

V2X 융합서비스 환경에서 지능형차량시스템의 위협 이슈

홍진근*
백석대학교 정보통신학부

Abstract In a V2X convergence service environment, the principal service among infotainment services and driver management services must be supported centering on critical information of the driver, maintenance manager, customer, and anonymous user. Many software applications have considered solutions to be satisfied the specific requirements of driving care programs, and plans. This paper describes data flow diagram of a secure clinic system for driving car diagnosis, which is included in clinic configuration, clinic, clinic page, membership, clinic request processing, driver profile data, clinic membership data, and clinic authentication in the V2X convergence service environment. It is reviewed focusing on security threat issue of ITS diagnostic system such as spoofing, tampering, repudiation, disclosure, denial of service, and privilege out of STRIDE model.

• Key Words : Smart car; Internet of Things; Secure; Threat; V2X

요 약 V2X 카 융합서비스 환경에서, 인포테인먼트 서비스와 운전자 관리 서비스 가운데 주요 서비스는 드라이버, 유지보수 관리자, 고객, 익명의 사용자의 중요한 정보를 중심으로 지원되어야 한다. 많은 소프트웨어 어플리케이션들이 운전 관리 프로그램과 계획의 특정 요구조건을 만족하기 위해 솔루션을 고려해오고 있다. 본 논문에서는 V2X 융합서비스 환경에서 클리닉 환경설정, 클리닉, 클리닉 페이지, 맴버십, 클리닉 요청 처리, 운전자 프로파일 데이터, 클리닉 맴버십 데이터 그리고 클리닉 인증을 포함한 운전자용 차량 진단을 위한 안전한 관리 시스템의 Data flow diagram을 설명하였다. STRIDE 모델 가운데 스푸핑, 탬퍼링, 부인방지, 노출, 서비스 거부, 권한 관리와 같은, ITS 진단 시스템의 보안 위협 이슈를 중심으로 고찰하였다.

• Key Words : 스마트 카; 사물인터넷; 안전한; 위협; V2X

1. Introduction

In the recent V2X convergence service trend according to high automation scenarios, it is issued to vehicle to x connectivity (which includes in two way communication between V2V and V2I), decision and control algorithms(for cooperative, safe, compatible traffic automation), digital infrastructure(which includes sourcing, quality control, and transmission), human factors(how humans interact with systems), evaluating road automation(public expenditure on supporting infrastructure or services), and

*교신저자 : 홍진근(jkhong@bu.ac.kr)
접수일 2015년 8월 25일 수정일 2015년 9월 18일 게재확정일 2015년 10월 20일

roadworthiness testing(deployment of new automated driving functionalities)[1]. Also about level of driving automation, the Society of Automotive Engineers (SAE) and Corporate Partnership Board (CPB) of International Transport Forum categories to human monitors environment and car monitors environment. The human monitors environment is from level0(no automation), to level1(driver assistance), level2(partial automation), and the car monitors environment is from level3(conditional automation), level4(high automation) to level5(full automation)[2].

Bharat bhushan Konka reviews a case study on software testing methods and tools in[3]. ISO 26262 safety standard supports to address the risk level for software characteristics of vehicles. ISO 26262 is consists of overall management of functional safety(part2), guideline(part10), automotive safety integrity level(ASIL)-oriented and safety-oriented analyses(part9), item definition/initiation of the safety lifecycle/hazard analysis & risk management/functional safety concept(part3), HW level(part5)/ SW level(part6) for product development(Safety validation, functional safety assessment, release for production), production/ operation/ servicing/ decommissioning (part7), planning for production and operation (part7). Donal Heffernan et. al. considered about verification review about ISO 26262 functional safety standard[4]. Torsten Schutze reviews automotive security, which is cryptolography for Car2X communication[5]. The security object for Car2X communication is presented security characteristics such confidentiality, integrity, availability, accountability, and authenticity[6]. Chapter 2 begins with a brief data flow in V2X clinic system, and in the Chapter 3, we have concluded in the research.

2. Data Flow in V2X Clinic System

2.1 DFD model in V2X Infrastructure

The diagnostic components of smart car have many car clinic information system applications. Moving information between disconnected systems limits the networked diagnostic ability of car clinic providers to collaborate efficiently in the delivery of car clinic information. The car clinic system utilizes variable applications for dictation, reviewing car diagnostic records, and other daily activities. Each inner car and control service center may maintain its own electronic database of car status information through network. These local data bases can then be connected via the network for clinic data transmission, so that service manager at one control center may review a connected car's status information from the information server. It is required, for the control manage implementation of IoT clinic environments, that a robust communication media be established that can transfer great amounts of data quickly and reliably. Smart car's private clinic privacy becomes an issue of concern when extra private information is collected besides IP location and GPS information for enhanced clinic contents. The car clinic portal solutions provide the foundation for more reasonable and efficient information sharing, enabling diagnosis professionals to work together more effectively, react more quickly, and deliver higher quality clinic in a wireless environment.

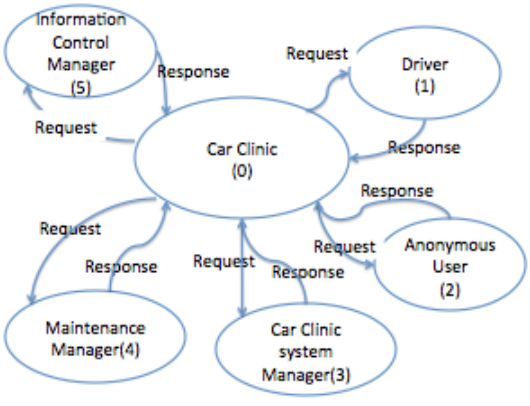
If the clinic software of smart car can detect an emergency state, the networked car clinic information manager will be notified and warned, the maintenance manager will be sent to examine the car status based on the information, and he will then decide on the best action for car clinic. The system is used to give feedback to the driver and the related user about the condition of the car's status, as well as about the status of the sensor components. The system can notify the emergency status of car, allowing the driver to report back a false alarm if one has occurred.

To design the secured car clinic service, first of all it must be defined what it is secured as follows questions : 1) what it is need to each parts of car clinic, 2) what/how use components, 3) what types of component properties.

Software services of car clinic require sufficiency of function requirements, tolerance of abnormal and malicious attacks, and corrective capability of software bugs. Vulnerability is often the weakness, which is searched and must be eliminated in the design of car clinic software. Threat defines how the vulnerability would be attacked, and if it is without vulnerability, it is no risk.

Driver executes login, response, and questions process, car clinic information control manager executes verify, preliminary question, generates tests and diagnosis and alert for connected car. Next, maintenance manager approve the diagnosis status of car. It is necessary for the DB to contain information including the owner name and number of the car, production date, and car clinic information manager in the higher layer, and, in middle layer, DB must maintain a list of attributes (car number, owner name, address, email ID, date of car production, etc).

The data flow diagram is following diagram, which shows interacts with car Clinic and external entities. The diagram shows the relation of a car driver, anonymous user, maintenance manager, and information control manager at a center with a number of car sensors that can communicate with a camera sensor, the diagnostic controller, and a RFID tag.



[Fig. 1] Data Flow Diagram of each elements such as Car Clinic, Car Clinic system Manager, Anonymous User, Driver, Information Control Manager

As a central control information hub, the car clinic portal service program can be tailored to the specific needs and roles of particular users such as driver, maintenance manager, and information control manager, providing instant access to proper applications, content, and services that promote collaboration and enhance community.

The relation of data flow types is illustrated as follows in <Table 1>.

〈Table 1〉 The basic data flow in each scheme

Shape	DFD type	Description
Painted circle	Complex process	Logical presentation of a pr process (service, daemon, assembly)
Single circle	Process	Logical presentation of a process (discrete task)
Rectangle	External entity	Something drives the application (users, event, process)
Parallel line	Data depository	File, DB
Arrowed line	Data flow	Data moves around system
Dotted line	Privilege boundary	m/m or process boundary, kernel/user mode code

In each DFD level, it shows one more complex process. It presents a hierarchical architecture and one element contains more elements through in each DFD level.

Element of Car Clinic is as follows:

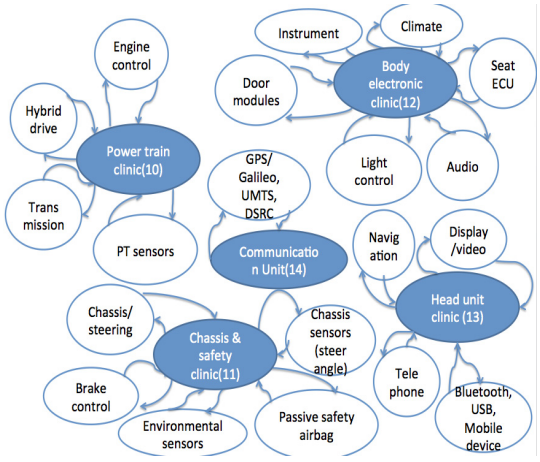
- *0.1 Car Clinic Configuration*
- *0.2 Car Clinic*
- *0.3 Car Clinic Page*
- *0.5 Driver profile*
- *0.6 Membership*
- *0.7 Car Clinic Request Processing*
- *0.8 Driver Profile data*
- *0.9 Car Clinic Membership data*
- *6.0 Car Clinic Authentication*

〈Table 2〉 The element of data flow diagram in car clinic application

Type of DFD element	DFD item
Entity	CCD(1.0), CCAU(2.0)
	CCSM(3.0), CCMM(4.0)
	CICM(5.0), CA(6.0)
Process	CCA(0.2), DP(0.5), M(0.6)
	CCRP(0.7.1), SCR(0.7.2)
	ACCR(0.7.3), DA(0.7.4), Q(0.7.5)
	LE(0.7.9)
Data Store	CCC(0.1), CCP(0.3)
	DPD(0.8), MD(0.9), CCR(0.7.6)
	ID(0.7.7), ACCR(0.7.8), AL(0.7.10)
Data Flow	CCCR(0.1 → 0.2)
	CCPR(0.3 → 0.2)
	AURR(2.0 → 0.2, 0.2 → 2.0)
	MRCU - CCCD(3.0 → 0.1, 0.1 → 3.0)
	MRCUD - CCP(3.0 → 0.3, 0.3 → 3.0)
	CCRCU - Request(0.2 → 0.7.1, 0.7.1 → 0.2)
	DRR(1.0 → 0.2, 0.2 → 1.0)
	MMRR(4.0 → 0.2, 0.2 → 4.0)
	ICMRR(5.0 → 0.2, 0.2 → 5.0)
	CARR(6.0 → 0.2, 0.2 → 6.0)

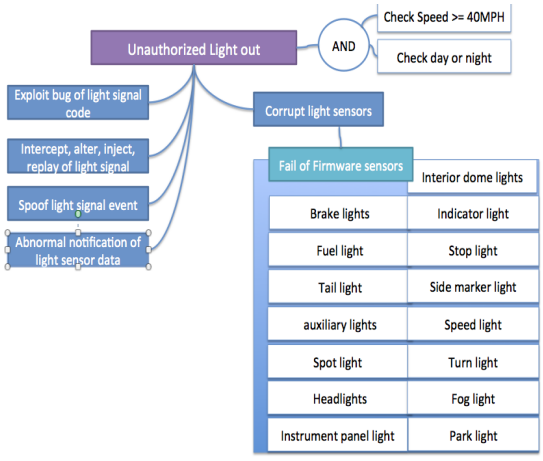
The entity is consists of Car Clinic Driver (CCD), Car Clinic Anonymous Users (CCAU), Car Clinic System Manager (CCSM), Car Clinic Maintenance Manager (CCMM), Car Information Control Manager (CICM), and Car Authentication (CAuth). The process is categories of Car Clinic Application (CCA), Driver Profile (DP), Membership (M), Car Clinic Request Processor (CCRP), Synchronous Clinic Request (SCR), Asynchronous Car Clinic Request (ACCR), Data Access(DA), Queuing (Q), and Logging Engine (LE). The Data Store is categories of Car Clinic Configuration (CCC), Car Clinic Pages (CCP), Driver Profile Data (DPD), Membership Data (MD), Car Clinic Request (CCR), Inventory Data (ID), Asynchronous Car Clinic Request (ACCR), and Audit Log (AL). The Data Flow is consists of Car Clinic Configuration Read (CCCR), Car Clinic Pages Read (CCPR), Anonymous User Request / Response (AURP), Manager Read, Create, Update (MRCU), Car Clinic Configuration Data (CCCD), Manager Read, Create, Update, Delete (MRCUD), Car Clinic Pages (CCP), Car Clinic Read Create, Update (CCRCU), Driver Manager Request/ Response (MMRR), Information Control Manager Request/Response (ICMRR), Car Authentication Request/Response (CARR).

The automotive on board network architecture of car infrastructure for diagnosis is reviews as follows in [Fig. 2][7]. It is sescribed use cases of V2x(V, I) communication, which is processed sending messages, safety reaction. Olaf Henniger et. al. suggests attack tree for unauthorized active braking such as corrupt CSC(exploit bugs, intercept/alter/inject/replay chassis-safety bus message, flash malicious code to firmware), spoof brake event in neighborhood(alter neighbor table, forward brake message from other neighborhood, brake notification from neighborhood on backbone bus), corrupt environment sensnrs(flash malicious code to firmware of environment sensors).



[Fig. 2] Data Flow Diagram of Network Architecture in Car Infrastructure

The abnormal status of light signal can be situated a extremely dangerous situation to driver. According to problem of light signal, it occurred to a various attack threats such as exploit bug of light signal code, intercept alter inject replay of light signal, spoof light signal event, abnormal notification of light sensor data, corrput light sensors as follows in [Fig. 3].



[Fig. 3] Light types and various light attack threats in V2X

2.2 Threats in the V2X communication [14,15]

We describe security threats in the respect of the STRIDE model.

1) Spoofing (GPS, position, ECU, Packet)

How to protect and authenticate in power train unit, communication unit, chassis & safety unit, body electronic, head unit? In a normal operation, it can be spoofed transmission packets in the vehicle bus by third party ECU [8].

2) Tampering(message, broadcasting)

How to assurance sufficient integrity, inspection, and evaluation of security performance out of internal devices in v2x infrastructure? For defense theft of cryptographic materials, it is needed to protect security information, which is supported resistance capacity with physical tampering. To countmeasure for tampering, it is considered revocation, short lived key, detection of malicious use of compromised keys [9]. Data tampering attack can destroy the network and causes dangerous consequence such as accidents [10,11].

3) Repudiation

How to guarantee signature problem and logging for v2x communication? This attack is out of lack of sufficient bus protection. How to maintain privacy of the vehicle and be able to solve the problem of non repudiation requirement. The security system of V2X must be supported non repudiation, which it can not be able to impossible to deny transmission of message between V-to-I, and V-to-V[12].

4) Disclosure

How to check and test from disclosure for v2x communication network? The anonymity is the related disclosure of the ID of the originator of messages generated by misbehaving or malfunctioning vehicles when traffic accidents[12].

5) Denial of service

How to control and chcek from excess abnormal consumption of v2x infrastructure resources such as CPU, memory, bandwidth, space, and time? Malicious attacker can be try to access connection from network serives such bluetooth, WiFi, DSRC, UMTS, and so on. Jamming attack is to disturbe vehicle from receiving data or primary key information.

6) Privilege

How to verify, debug, and consider the problem of privilege against corruption? The private vehicle may pretend to be public role vehicles such as emergency vehicles, to gain privileges and also it tries to gain high privilege over the road[13].

3. Conclusion

This paper describes data flow diagram of a secure clinic system for driving car diagnosis in the V2X service environment. It is reviewed focusing on security threat issues such as spoofing, denial of service, tampering, repudiation, disclosure, and privilege on the related of ITS diagnostic system. It is described type of DFD element, which is focusing on entity, process, data store, and data flow. The car clinic

communicate with information control manger, driver, maintenance manager, car clinic system manager, and anonymous user in data flow diagram of each elements.

ACKNOWLEDGMENTS

본 논문은 백석대학교 산학협력단의 지원을 받아 수행된 것임

REFERENCES

[1] Corporate Partnership Board, Automated and Autonomous Driving Regulation under uncertainty, International Transport Forum, 2015.

[2] SAE Standard J3016, 2014.

[3] Bharat Bhushan Konka, "A Case study on Software Testing Methods and Tools - A pre study on software testing requirements of ISO/DIS 26262," MS dissertation, University of Gothenburg. 2011.

[4] Donal Heffernan, Ciaran MacNamee, Padraig Fogarty, "Runtime verification monitoring for automotive embedded systems using the ISO 26262 functional safety standard as a guide for the definition of the monitored properties," IET software, Vol. 8 Issue. 5, pp. 193-203, 2014.

[5] Torsten Schutze, "Automotive Security: Cryptography for Car2x communication," Embedded World Conference, 2011.

[6] ETSI TR 102 893, Intellignet Transport Systems (ITS); security, threat, vulnerability and risk analysis (TVRA), 2010.

[7] Olaf Henniger, Ludovic Aprille, Andreas Fuchs, Yves roudier, Alastair Ruddle, Benjamin Weyl, "Security requirements for automotive on board networks," IEEE ITST, 2009.

[8] Karl Koscher, "Security Embedded Systems: Analyses of Modern Automotive systems and enabling Near Real Time Dynamic Analysis," PHD dessertation, University of Washington, 2014.

[9] National Highway Traffic safety Administration, Vehicle Safety Communications - Applications (VSC-A) Final report : Appendix Vol. 3 Security, DOT HS 811 492D, 2011.

[10] Elyes Ben Hamida, Hassan Noura Wassin Znaidi, "Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures," Electronics, pp. 380-423, 2015.

[11] Zeadally, s., Hunt R., Chen Y. S., Irwin A., Hassan A., "Vehicular ad hoc networks (VANETS): status, results, and challenges," Telecommun. Syst. Vol. 50, pp. 21-241, 2012.

[12] http://www.syssec-project.eu/m/page-media/3/sys sec-d6.2- SecurityOfTheConnectedCar.pdf.

[13] Liting Huang, "Secur and Privacy Preserving Broadcast Authentication for IVC," MS thesis, Distributed and Embedded Security Group, Mathematics and Computer Science, Universiteit Twente, 2012.

[14] Hendrik Schweppe, Yves Roudier, "Security issues in vehicular systems : threats, emerging solutions and standards," SAR-SSI2010, 5th Conference on Network Architectures and Information Systems Security, pp. 18-21, 2010.

[15] Karyn Hodgson, "The internet of security things," Integration & Networking Solutions, Vol. 45, Issue. 9, pp. 54-72, 2015.

저자소개

홍 진 근(Jin-Keun Hong) [정회원]

- 1991년 2월 : 경북대학교 전자공학과 (공학사)
- 1994년 2월 : 경북대학교 전자공학과 (공학석사)
- 2000년 2월 : 경북대학교 전자공학과 (공학박사)
- 2004년 3월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야> : 융합망, 융합보안, 개인화 보안