Research on cyber security Technology and Test Method Of OTA for Intelligent Connected Vehicle

He Kexun
CATARC Automotive Test Center (Tianjin) Co., Ltd, TATC
Tianjin, China
hekexun@catarc.ac.cn

Wang Changyuan
CATARC Automotive Test Center (Tianjin) Co., Ltd, TATC
Tianjin, China

Han Yanyan
CATARC Automotive Test Center (Tianjin) Co., Ltd, TATC
Tianjin, China

Fang Xiyu
CATARC Automotive Test Center (Tianjin) Co., Ltd, TATC
Tianjin, China

***Abstract*—As the development of automotive intelligent and networking, OTA technology has become an important means of remote upgrade of connected cars. However, cyber security problems have not been solved in the OTA upgrade process of the connected cars. The lack of data protection strategy and testing methods seriously hinder the application of OTA upgrade. This paper takes the typical connected car OTA upgrade system architecture as a case and analyzes the architecture and upgrade process of the connected vehicle OTA upgrade system. And this paper researches the cyber security threat model of the OTA upgrade systems. This paper proposes an all-around protection strategy for OTA upgrade system cyber security of connected vehicle. This paper proposes a comprehensive and implementable test evaluation method basing on the professional darkroom. The results provide reference for OTA-based intelligent connected vehicle.**

Keywords- Intelligent Connected Vehicle; OTA;cyber security; Assessment and test method

I. INTRODUCTION

Automotive OTA (Over-The-Air) upgrade, also known as over-the-air upgrade, refers to remote management of terminals and applications through the air interface of mobile communications. OTA technology can be understood as a remote wireless upgrade technology [1]. With the development of automotive intelligent and networking, cars not only assume functions of body control, electronic and electrical system control, and cloud-side information interaction, but also provide a wealth of infotainment services for vehicle users [2]. Correspondingly, the vehicle's electrical structure is becoming more complicated with more software and hardware. As the iteration speed of intelligent and networked technologies accelerating, the complexity of electrical systems brings greater maintenance costs. The update frequency software and hardware update frequency of intelligent connected cars is increasing. In order to solve problems of operation and maintenance and cost caused by frequent updating of software and hardware, and to provide more convenient upgrade services for automobile users, OTA has become an important way for remote upgrades of automobiles. The industry generally believes that the OTA upgrade technology of intelligent connected cars is the future development trend [3,4].

However, while the automobile OTA upgrade provides an important update path for intelligent connected cars, it also brings more confidence and security risks. In recent years, the cyber security incidents of connected cars such as JEEP and Tesla have aroused widespread concern [5,6,7]. OTA upgrades provide internal and external interconnection interfaces. The upgrade process requires the download of upgrade packages and firmware and software updates, bringing information security risks to vehicles [8].

Recently, Tesla, Toyota, Ford, Volvo and other manufacture are actively deploying automotive OTA upgrade technology [4]. Although the United Nations WP.29, the United Kingdom, and China have begun to formulate standards and regulations related to automotive OTA upgrade, at present, the application of OTA upgrade for connected cars is still in the realization of functions stage. It lacks consideration and layout of cyber security. The lack of test and evaluation method specifically for the OTA upgrade information security of connected cars, brings new difficulties to the remote upgrade security of intelligent connected cars [9,10].

In view of this, this article investigates and analyzes the existing OTA upgrade architecture. This study researches the threats faced by OTA upgrade, and proposes a response solution. Relying on the special darkroom, this study researches the test evaluation method of automobile OTA upgrade, and proposes a test evaluation method. To provide support for the automotive industry of OTA upgrade cyber security, this paper provides test verification of OTA upgrade cyber security.

978-1-7281-6499-1/20/$31.00 ©2020 IEEE
DOI 10.1109/ICBAIE49996.2020.00048

II. ICV OTA ARCHITECTURE AND THREAT ANALYSIS

A. Analysis of OTA Upgrade Architecture of Connected Car

The vehicle OTA system includes the service platform side and the vehicle side [13]. The service platform and the vehicle communicate with each other through 4G or Wifi. The service platform and the vehicle adopt a one-to-many approach. The service platform is a private cloud service platform deployed in the data center. Only the CDN (content distribution technology) is used to implement simultaneous updates of vehicles located in different areas [12]. Figure 1 shows a typical OTA system architecture case.

In the case, the OTA system consists of a service platform and a vehicle. The service platform mainly consists of six parts: OTA upgrade system service sub-platform, TSP service platform, differential service sub-platform, version management sub-platform, security service sub-platform and CND. Among them, the platform side communicates with the vehicle side through the TSP service sub-platform and CND. The TSP platform is responsible for performing message interaction with the vehicle-side end for issuing upgrade instructions. CDN (Content Distribution Network) caches the contents of the upgrade package to the border gateway of the mobile network [11], supports the distribution of resources through the wireless network, and provides upgrade package download services.

The on-vehicle side consists of an upgrade management side and an upgrade client. Among them, the upgrade of the ECU is directly performed by the upgrade management side of the vehicle. The upgrade management side runs on the TBOX or the MPU of the gateway, and assumes the role of diagnostic instrument refresh and the node ECU refresh traditional UDS service. MPU systems other than the ECU are upgraded using the upgrade client. The internal connection of the vehicle is mainly through USB and on-board Ethernet. The upgrade management end of the vehicle plays the role of in-vehicle end support in the entire OTA upgrade system. On the one hand, it communicates with the OTA service platform to obtain upgrade information. On the other hand, it provides upgrade information to other ECUs and upgrade clients and controls them for safe upgrades.

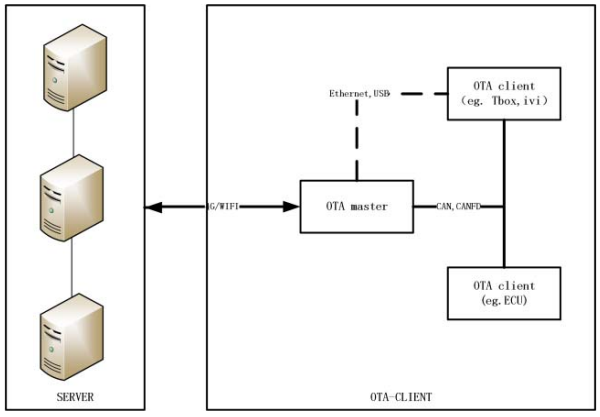

Figure 1 Typical OTA upgrade system architecture

Connected car OTA upgrade process:

1) Update package upload. After generated basing on update requirements, the update package contains bug fixes or new features, update sequences, verification checks, and more. After the update package is generated, upload it to the service platform.

2) Vehicle version is reported. After the vehicle powering on, it will communicate with the TSP sub-platform on the service platform side. The vehicle side collects the software version information of all the controllers inside the vehicle, and then reports it to the service platform through the communication link.

3) Version comparison. The version information reported by the vehicle side is compared with the version information of the service platform side. If a newer version exists on the service platform side, the service platform side will form an update message to be issued.

4) Push update message and download URL. The service platform pushes the update prompt and update package download URL to the vehicle through the TSP service sub-platform. After receiving the update message, the user can choose to update or not update.

5) Confirm the download. After receiving the update message pushed by the service platform, the user chooses to download the update package.

6) Download resource packs. The vehicle user receives the update message and download URL to confirm the upgrade. Then, OTA system establish a connection between the URL service platform and the vehicle.

7) Download the upgrade package. The service platform downloads the upgrade package to the vehicle through the CDN.

8) Start the upgrade. When the vehicle detects that the vehicle is in an upgradeable state, the download update package will be officially updated, replacing the old version with a new image file.

9) Report the upgrade status. The entire process will be monitored in real time for updates, and the update status will be reported to the service platform through TSP.

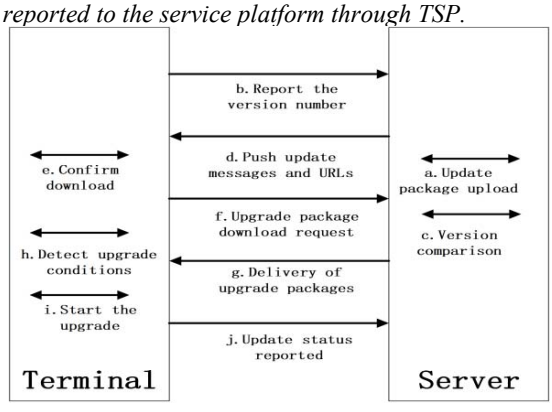

Figure 2 OTA upgrade process.

B. *Analysis of cyber Security Threat of OTA Upgrade for Connected Cars*

During the OTA upgrade process of Connected Cars, transmission risks and tampering risks of upgrade packages are the main cyber security threats faced by OTA system. There are cyber security risks from the service platform to the message, the data transmission channel to the vehicle. First of all, there have loopholes in the system on the service platform side, the development port, and the various sub-platform systems and databases, which become the entrance to hacking. During the data transmission process, the messages that the service platform and the vehicle interact with may be hijacked and forged. In the transmission process of downloading the upgrade package on the vehicle side, the attacker can use network attack methods, such as man-in-the-middle attacks, to send the falsified upgrade package to the vehicle side.

If the terminal also lacks a verification mechanism during the upgrade process, the tampered upgrade package may replace the correct upgrade package to complete the upgrade process, achieving the purpose of tampering the system and implanting malicious programs such as backdoors. An attacker may also perform unpacking analysis on the upgrade package to obtain some available information, such as vulnerability patches. The exposure of key information in the upgrade package will increase the risk of being attacked. Attackers use remotely upgraded protocol defects, such as firmware verification, missing signatures, server forgery, etc., to flash and tamper with software and firmware, thereby attacking intelligent connected cars. In addition, the attacker attacked the communication network link when the connected car was known to be remotely upgraded, preventing the connected car from installing an update and repair system.

III. CONNECTED CAR OTA UPGRADE INFORMATION SECURITY STRATEGY

Whether it is ISO26262, J3601 of the American Society of Automotive Engineers or PAS1885 of the United Kingdom, Connected Cars is required to manage automotive cyber security from the perspective of the entire life cycle. Therefore, the information security of the car should be ensured during each upgrade process. In view of the current popularity of vehicle information security technology, OTA upgrades should be from a system perspective, including identity authentication, access control, data security, communication protocols, code security, diagnostic refresh security, and human-computer interaction security. In formulating a protection strategy, the information security risks involved in the transmission process and the tampering information security risks involved in the upgrade package should be fully considered. Specific protective measures are shown in Table 1.

TABLE I. SECURITY PROTECTION STRATEGY

Protection type	Protection strategy
Authentication	Two-way identity
	Support HSM
	Special secret key
Data security	no upgrade information in memory
	Local Data storage security
	Data Integrity
	Debugging cyber security
	security log
Man-machine interaction	Prevents prompt window from responding repeatedly
Access concrol	Upgrade package sits with access control
communication security	Encrypted transmission should be taken
	Communication protocol anti-replay
	Communication protocol tamper-proof
code security	Code confusion anti-reverse
Upgrade security	Upgrade package transport integrity
	Upgrade package data signature
	Upgrade process authentication

IV. INTERNET-CONNECTED AUTOMOTIVE OTA UPGRADE INFORMATION SECURITY TEST METHOD

A. *Testing environment*

The connected car OTA system involves the information interaction between the service platform and the vehicle. In order to ensure that the daily operations of the service platform are not affected and to avoid public network security issues during the test, the test environment needs signal shielding. In this study, after comparing the test environments of shielded rooms, signal shields and dark rooms, we chose to perform the OTA system information security test in a dedicated dark room environment. The specific test environment is shown in the figure:

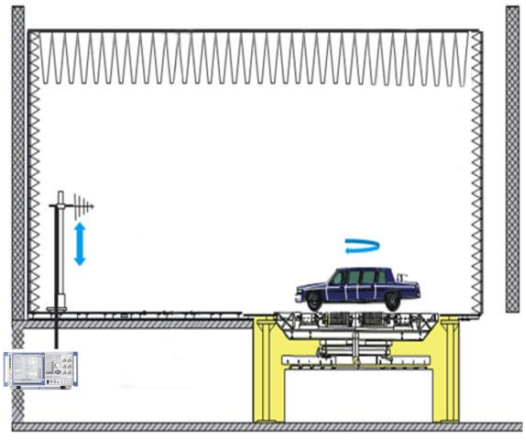

Figure 3 Testing environment

First, the test environment is divided into a vehicle darkroom and a test area. The test area contains the tester's penetration test analysis area, test industrial control equipment, and simulation platform. The test industrial control equipment is connected to a simulated base station in a vehicle dark room through a dedicated network. The simulated base station simulates the connection between the 2G / 3G / 4G and wifi

networks in the public network and the vehicle, and Chase tests the communication between the industrial control equipment and the OTA system vehicle. Penetration test test cases required for the design test issued by industrial control equipment.

B. *Testing process*

Networked car OTA system test includes 7 parts: preliminary public opinion collection, threat analysis, risk grading and evaluation, penetration test, evaluation, retest, and test report. First of all, in the public opinion collection part, the latest authoritative vulnerability libraries, materials, and the latest automotive information security events and vulnerabilities in the literature are collected. In the threat analysis phase, by analyzing the architecture and technology of the vehicle under test and the OTA system, the threat of vehicle OTA upgrade is studied and a threat model is constructed. After the threat model is established, the level determination and risk assessment of the threat model are performed through risk grading and evaluation. The important work in the risk grading stage is to review and verify the protection strategies adopted by the system.

Penetration testing mainly tests the security of OTA upgrades from the perspective of an attacker. Penetration testing includes test case design, simulated attacks and vulnerability analysis. The use case design relies on the test plan to design penetration test cases that can be used for operation. The testers rely on the test cases to simulate the attacks. For the discovered vulnerabilities, the testers use the simulation simulator to perform vulnerability playback and analysis. After the penetration test, the results of the penetration test must be analyzed to form a penetration test report containing suggestions for bug fixes. After the penetration test is completed, the OTA system information security is evaluated based on the comprehensive test results, and a test evaluation report is obtained.

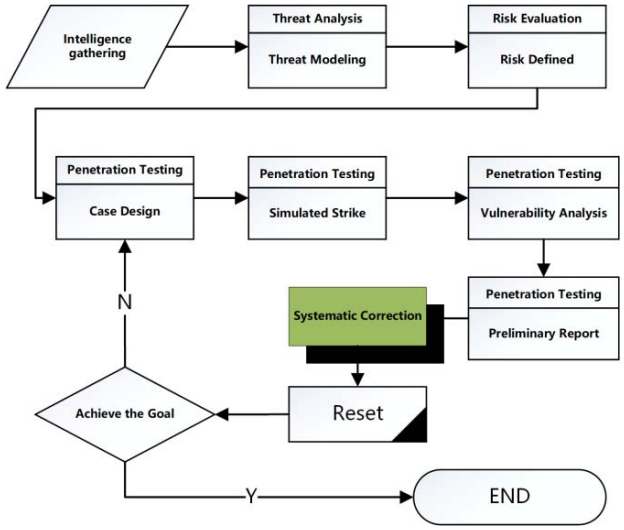

Figure 4 Testing process

C. *Evaluation System*

The score of OTA system upgrade security is calculated from six perspectives: identity authentication, data security, access control, communication security, code security, upgrade security, and human-computer interaction security.

The weight of each information security item is shown in Table 2:

TABLE II. EVALUATION WEIGHT

Protection type	Protection strategy
Authentication（19%）	Two-way identity（30%）
	Support HSM（40%）
	Special secret key（30%）
Data security（17%）	no upgrade information in memory（25%）
	Local Data storage security（30%）
	Data Integrity（20%）
	Debugging cyber security（15%）
	security log（10%）
Man-machine interaction（5%）	Prevents prompt window from responding repeatedly（100%）
Access concrol（10%）	Upgrade package sits with access control（100%）
communication security（18%）	Encrypted transmission should be taken（40%）
	Communication protocol anti-replay（30%）
	Communication protocol tamper-proof（30%）
code security（5%）	Code confusion anti-reverse（100%）
Upgrade security（24%）	Upgrade package transport integrity（20%）
	Upgrade package data signature（40%）
	Upgrade process authentication（40%）

Each evaluation category has different percentage weights. Each evaluation category contains different evaluation items, and each evaluation item has different percentage weights. The score of the evaluation item is calculated according to the percentage system. The calculation method is to multiply the score of the test item by the weight percentage corresponding to the test item and the weight percentage of the test category to which it belongs:

$$S_i = SWiV_i$$

In the formula, Si is the score of the i test item, Wi is the weight of the test class where i is, and Vi is the weight of the i test item.

The score of the OTA information security evaluation of the connected car is the sum of the scores of all the test items. Total score calculation formula:

$$S_{total} = \sum_{i=1}^{n} S_i W_i V_i$$

In the formula, i is the serial number of the test category, Total is the total information security score of the OTA system, Si is the score of each test item i, Wi is the percentage weight of the test item i, and Vi is the percentage weight of the broad category of the test item i.

V. CONCLUSION

Through in-depth research on the composition and upgrade process of the connected vehicle OTA upgrade, this article analyzes cyber security threats faced by the OTA upgrade of the connected car. Based on the intelligent connected vehicle cyber security technology, OTA upgrade cyber security protection measures are proposed, from the perspectives of data security and communication security. Fully considering the environment and process specificity in the OTA upgrade cyber security test, a method for testing and evaluating of the OTA upgrade cyber security of a networked car basing on a professional darkroom is provided.

REFERENCES

[1] SHI JUN-fang, LI Xiao-jiang, MEI Luan-fang, "Design of Remote Trusted Upgrade for Embedded Terminal" [D]. 2010.

[2] LI Keqiang, DAI Yifan, LI Shengbo, BIAN Mingyuan, "State-of-the-art and technical trends of intelligent and connected vehicles"[J], Automotive Safety and Energy, 2017, 8(1): 1-14.

[3] GAO Jie, WANG Qing, "A Design Scheme of OTA Upgrade Service Platform for Electric vehicles", Computer Knowledge and technology, 2017 (8): 89.

[4] Wu Xiangyu, Zhao Dehua, Hao Tieliang, " Analysis on current situation and future development trend of vehicle OTA", Automobile Applied Technology". 2019, 3:1671-7988.

[5] A. Bouard, M. Graf and B. Burgkhardt, "Middleware-based security and privacy for in-car integration of third-part applications", 401:17-32,2013.

[6] I. Symeonidis, M. Mustafa and B. Preneel, "Keyless car sharing system: A security and privacy analysis", in Proc. IEEE 2nd International Smart Cities Conference: Improving the Citizens Quality of Life (ISC2 2016), 2016.

[7] T. Becsi, S. Aradi and P. Gaspar, "Security issues and vulnerabilities in connected car systems", in Proc. 2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS 2015), pp. 477-482, 2015.

[8] Shi yong, "Research and Implementation of Remote Upgrade Security Mechanism for Vehicle Terminal System"[D], Hebei University of Science and Technology, 2016.

[9] Zhang HaiChiang"Research and Implementation of Intelligent Remote Upgrade Techology for Intelligent Network Connection Vehicles", University of electronic Science and technology of China, 2018.

[10] Yang M, Zhu F. The Design of Remote Update System Based on GPRS Technology[C] Management and Service Science (MASS), 2010 International Conference on. IEEE, 2010:1 - 4.

[11] Zhu Xipeng, "Research on Key Techologies of Mobile Content Distribution"[J], Beijing University of Posts and Telecommunications, 2018.

[12] Wang Dongliang, Tang Lishun, Chen Bo, "The Research of OTA Function Design for Intelligent Connect Vehicle"[J], Automobile Technology, 2018: 29-33.

[13] Sun Jianke, "Research of Differential Files and Compression Algorithm Based on FOTA"[J], Xidian University 2014.