Research on Safety Testing Technology of IVI Based on the bypass of Unilateral Authentication

Jinchao Zhang[1,2,a], Xia Liu[1,2,b], Qi Li[1,2,c], Yujiao Wang[3,d], Yanyan Han[1,2,e]

[1]CATARC Software Testing (Tianjin)Co.,Ltd. ,Tianjin 300000,China;

[2]CATARC Automotive Test Center (Tianjin) Co.,Ltd., Tianjin 300000,China;

[3]School of Naikai University, Tianjin 300000, China;

[a]zhangjinchao@catarc.ac.cn, [b]castc_liuxia@163.com, [c]liqi2019@catarc.ac.cn,
[d]2108140943@qq.com, [e]hanyanyan@catarc.ac.cn

Abstract

IVI through wireless network and external network connection, and information transmission, this process will face the authentication of security issues. Most apps in IVI adopt unilateral authentication technology to complete authentication communication. In order to understand the principle of unilateral authentication communication technology and test the security of unilateral authentication of the system, a research on unilateral authentication bypassing security testing technology of IVI was proposed. The research contents are mainly divided into the following aspects: With SSL/TLS unilateral authentication technology, SSL Pinning technology, JustTrustMe certificate bypass technology, and using tools such as Wireshark, Fiddler, Xposed+JustTrustMe, ADB, it aims to complete the security test practice of unilateral authentication on vehicle entertainment systems.

Keywords

IVI; JustTrustMe; the bypass of unilateral authentication.

1. Introduction

The IVI, also known as IVI, is a device that uses various communication internet technologies to support the information exchange between the automotive intranet and the external network, thereby achieving services such as remote query, information entertainment and other services.It is undeniable that the emergence of the IVI not only enhances travel safety and travel experience, increases driving pleasure, but also brings various convenience to people’s lives.0

However, with the increasingly intelligent vehicle information entertainment system, the information security issues brought by it are becoming increasingly severe.A series of information security incidents such as Toyota Motor's second data leakage and the warning of "gunfight on the road" in some brands of cars in Shanghai are reminding us: this system involves many aspects such as software, communication, and data, in particular, during operation, it will connect with the external network through cellular or wireless network, and carry out information transmission. In this process, many security issues such as encryption, certification, and protocols will be faced.

Identity authentication is the first line of defense of network information security. In the IVI, in order to reduce the pressure on the server side and verify the legitimacy of the identity, most of the APP applications use SSL Pinning technology. In order to test the security of this technology,this article will start from the principle of this technology, analyze and propose the bypassed strategy, and complete the practice that SSL Pinning in the IVI is bypassed.

2. SSL/TLS Unilateral Authentication Process

As shown in Figure 1, the general process of SSL/TLS unidirectional authentication for the built -in APP and server of the IVI.

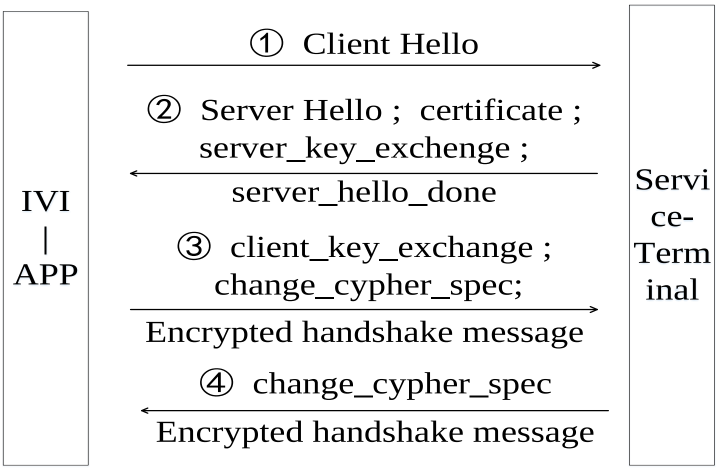


Figure 1: SSL/TLS Unilateral authentication process

2.1. The built-in APP of the IVI initiates a request from the server side:

Client hello：Including the list of the highest SSL/TLS protocol version, password kit (mainly includes password exchange algorithms, signature authentication algorithms, symmetrical encryption algorithms, message abstract algorithms)(Cipher Specs), and random number A generated by the client, which is used to generate the "session key" later.

2.2. The server responds to the built-in APP of the IVI:

Server hello：Including the SSL/TLS protocol version and password kit determined to be used, random number B generated by the server, later used to generate "session keys" and session ID.

Certificate：Electronic version certificate in the server secret library.

Server key exchange：The key exchange process, the key negotiation algorithm used before the APP and the server set up communication is DHE/ECDHE, which is sent here the DH parameters used by the server.

Server hello done：It shows that the server completes message transmission.

2.3. The built-in APP of the IVI responds after receiving the reply from the server:

Check the server certificate. If the verification is not passed, the link is disconnected; if the verification is passed, the response message is returned.

Client key exchange：If it is an RSA algorithm, a random number Pre-Master Secret will be generated, and then the public key is encrypted with the public key on the server，and then put into the packet. If the DH algorithm is used, the DH parameter is sent to the client. Then the server and the client calculate the same pre-master secret according to the DH algorithm;

Change cipher spec：The server notifies the APP to start sending packets in encrypted mode. The client uses the above 3 random numbers A, B, Pre-Master Secret, and the negotiated algorithm to calculate the key to the symmetrical encryption algorithm;

Encrypted handshake message：The previously sent data is summarized, encrypted, and verified by the server.

2.4. Server-side response APP message:

Change cipher spec： The server notify the app to start sending messages using encryption. The server uses the above 3 random numbers A, B, Pre-Master Secret, and the negotiated algorithm to calculate the key to the symmetrical encryption algorithm;

Encrypted handshake message： The previously sent data is summarized, encrypted, and verified by APP.

3. The built-in APP of the IVI adopts the SSL Pinning mechanism

Under normal circumstances, the APP verification server certificate mainly includes the following four aspects:

Credibility of certificate: Whether the verification certificate is issued by the trusted CA root certificate authority. In order to ensure that the server obtained by the client is not tampered with, the authoritative third -party CA agency is required.CA agencies are responsible for verifying the information of the public key owner, issuing certificates (signing the server public key), and providing certification verification services for users.

Certificate revoked: Whether the verification certificate is valid。 The CA institution can issue a certificate, but it can also invalidate previously issued certificates. If the subject of the certificate appears: the private key is lost, the application certificate is invalid, etc., the CA agency needs to abandon the certificate.

Certificate expires: Whether the validity period of the verification certificate has expired: whether the Validity Period field in the main judgment certificate expires.

Certificate domain name: Verify whether the domain name of the certificates is consistent: Check whether the domain name of the certificate matches the current access domain name.

Certificate verification checks whether the certificate expires, whether the domain name on the server certificate matches the actual domain name of the server, and verifies the certificate chain. The verification is relatively weak.

Therefore, after the Fiddler generates an intermediate certificate, put the intermediate certificate under the system certificate path, and Fiddler can use Fiddler to achieve intermediate people attack.

SSL Pinning, SSL certificate binding technology. After OEM completes the development test on the APP, it is bound to the designated certificate to the corresponding APP program. The app only accepts communication data of the designated certificate. In this way, even if the fiddler's middleman certificate is placed under the system certificate path, the application is also Do not trust the Fiddler's certificate, thereby interrupting the connection with the server.

SSL Pinning has two ways: certificate lock and public key lock.

Certificate lock: Need to accept a certificate of the specified domain name on the client code, not any certificate built in the operating system, through this authorization method, the uniqueness and security of APP and server communication are guaranteed. therefore, communication between clients and server-side can ensure absolute security. However, the validity period of certificates issued by CA exists. The disadvantage is that the certificate needs to be re-built into the APP after the certificate is renewed.

Public key lock: Extract the public key in the certificate and built into the client to verify the correctness of the connection by comparing the public key value with the server. When making a certificate key, the public key can remain unchanged before and after the renewal of the certificate (that is, the key to the same), so it can avoid the issue of the validity period of the certificate.

4. JustTrustMe Unilateral Authentication Bypass the Principles and Process Analysis

4.1. JustTrustMe principle

JustTrustMe attempts to solve the Pinning problem by hook all the API verifying SSL certificates during the above verification process to bypass the certificate check (returning true or not allowing it to be verified at all).

For the SSL certificate verification in OKHTTP, CertificatePinner (certificate lock) will call the check method for the certificate verification; HostnameVerify, the default call HostnameVerifier. verify for server hosting verification, or the custom HostnameVerify default calls of the custom HostnameVerifier. verify for verification.JustTrustMe requires the class name and method name corresponding to hook.

For the verifications of DefaultHttpClient and SSLSocketFactory, JustTrustMe focuses on the hook parameter ClientConnectionManager and TrustManager to trust any certificate.

For the SSL certificate verification in HttpsURLConnection, JustTrustMe requires to Hook getTrustManager method, setDefaultHostnameVerifier method, setSSLSocketFactory method and setHostnameVerifier method, to trust any certificate.

For the certification verification of the HTTPS page through WebView in the Android system, the certificate verification fails, and stop loading the page. JustTrustMe requires to hook the processing method of WebView certificate verification failure onReceivedSslError, so that webview can continue to load the webpage.

4.2. Unilateral certification bypass process analysis

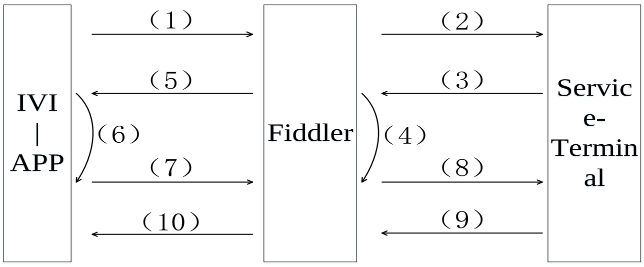


Figure 2: Unilateral authentication bypasses

(1)The built-in APP sends a request to the server side (Fiddler certificate is built into the system certificate directory, the IVI is configured with the Fiddler side proxy IP and port number) contains TLS/SSL protocol versions, encryption algorithm kits, and random A.

(2)The APP request to the server side by Fiddler;

(3)The SSL/TLS protocol version, password kit and CA certificate used by the server side;

(4) Fiddler intercepts the CA certificate on the server, decrypts it with the root certificate public key, verifies the server data signature, and obtains the CA certificate public key of the server. And forged their own credentials.

(5)Fiddler conveys its own forgery certificate to the built-in APP of the IVI;

(6) The built-in APP of the vehicle entertainment system checks the obtained forged certificate (JustTrustMe played a role in the process, and the API of all verification SSL certificates was hooked), and the forged certificate passes the verification successfully. The built-in APP obtains the forged certificate public key (false public key). Then the pre-master secret is generated and the pseudo-symmetric key is calculated;

(7)Pass to the server after encrypted Pre-Master Secret with a fake public key, which is intercepted by Fiddler;

(8)Fiddler unlocked the intercepted ciphertext with the private key of its own falsification certificate, obtained the Pre-Master Secret, and calculated the true symmetrical key.Pass the Pre-Master Secret with a server certificate and public key encryption to the server. The server uses a private key to calculate the true symmetry key;

(9)The handshake is completed. The packets encrypted by the server with the true-symmetric key are then intercepted by Fiddler. The packets are decrypted with the true-symmetric key and then encrypted with the false symmetric key. The packets are then sent to the app, which decrypts the packets with the false symmetric key and gets the plaintext;

(10)Complete handshake.

5. Verification by experiment

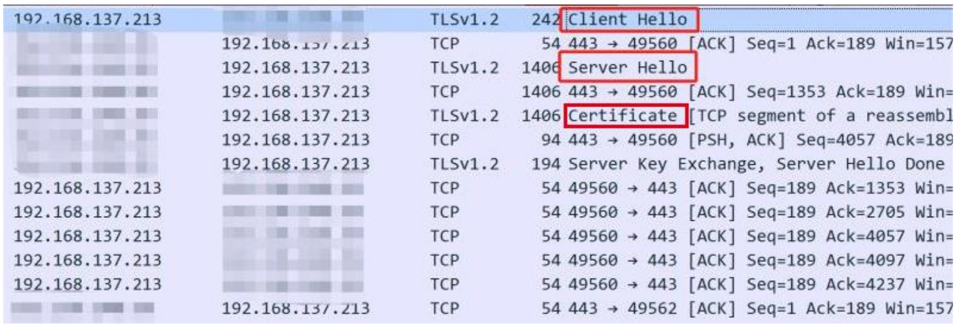
Test the built-in weather forecast APP built by the IVI:

Preparation:Install Wireshark, adb, Fiddler on the computer used in the experiment（configuration：Export the root certificate and place it in the system directory、Capture HTTPS CONNECTS、Allow remote computers to connect）；Install the Xposed framework on the IVI, as well as the JustTrustMe module and restart.

Step 1:Use wireshark to capture packets and determine whether the SSL/TLS handshake process in the IVI is unilateral authentication.

When the IVI connects to the computer hotspot, start Wireshark software on the computer to monitor the corresponding network adapter and enable packet capture. Start and close the weather forecasting app several times to determine the corresponding SSL/TLS protocol handshake process when the software is started.

As shown in Figure 3, the Server sends a certificate file after sending the Server Hello. APP authenticates the server, but the server does not authenticate the APP. Therefore, the current communication is unilateral authentication communication.



```
192.168.137.213  [redacted]       TLSv1.2   242 Client Hello
[redacted]       192.168.137.213  TCP        54 443 → 49560 [ACK] Seq=1 Ack=189 Win=157
[redacted]       192.168.137.213  TLSv1.2  1406 Server Hello
[redacted]       192.168.137.213  TCP      1406 443 → 49560 [ACK] Seq=1353 Ack=189 Win=
[redacted]       192.168.137.213  TLSv1.2  1406 Certificate [TCP segment of a reassembl
[redacted]       192.168.137.213  TCP        94 443 → 49560 [PSH, ACK] Seq=4057 Ack=189
[redacted]       192.168.137.213  TLSv1.2   194 Server Key Exchange, Server Hello Done
192.168.137.213  [redacted]       TCP        54 49560 → 443 [ACK] Seq=189 Ack=1353 Win=
192.168.137.213  [redacted]       TCP        54 49560 → 443 [ACK] Seq=189 Ack=2705 Win=
192.168.137.213  [redacted]       TCP        54 49560 → 443 [ACK] Seq=189 Ack=4057 Win=
192.168.137.213  [redacted]       TCP        54 49560 → 443 [ACK] Seq=189 Ack=4097 Win=
192.168.137.213  [redacted]       TCP        54 49560 → 443 [ACK] Seq=189 Ack=4237 Win=
[redacted]       192.168.137.213  TCP        54 443 → 49562 [ACK] Seq=1 Ack=189 Win=157
```

Figure 3: The Wireshark captures packets

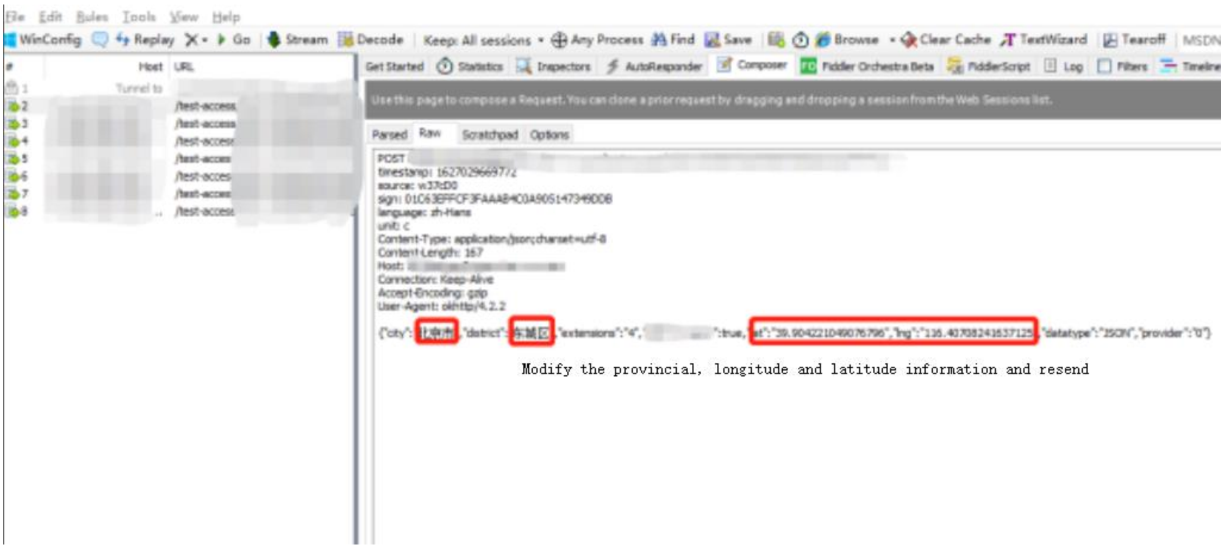
Step 2: Modify the IVI agent ip and port, use Fiddler to capture the package.

Run adb connect IP1:5555 and adb shell settings put global http_proxy IP2:8888 on the terminal command line to set the IVI proxy to ports IP2 and 8888. IP2 is the IP address corresponding to Fiddler.

Open Fiddler and open the weather forecast APP. You can view the plaintext data in the communication process in Fiddler.

Step 3: Modify the parameters of the intercepted packet and send it to the server to verify whether the server has verification.

Click Composer: Modify the latitude and longitude parameter values to Dongli District of Tianjin (see Figure 4), and click Execute to request again.


File Edit Rules Tools View Help
WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN
Get Started Statistics Inspectors AutoResponder Composer Fiddler Orchestra Beta FiddlerScript Log Filters Timeline
Use this page to compose a Request. You can clone a prior request by dragging and dropping a session from the Web Sessions list.
Parsed Raw Scratchpad Options
# Host URL
1 Tunnel to
2 /test-access
3 /test-access
4 /test-access
5 /test-acces
6 /test-acces
7 /test-access
8 /test-acces

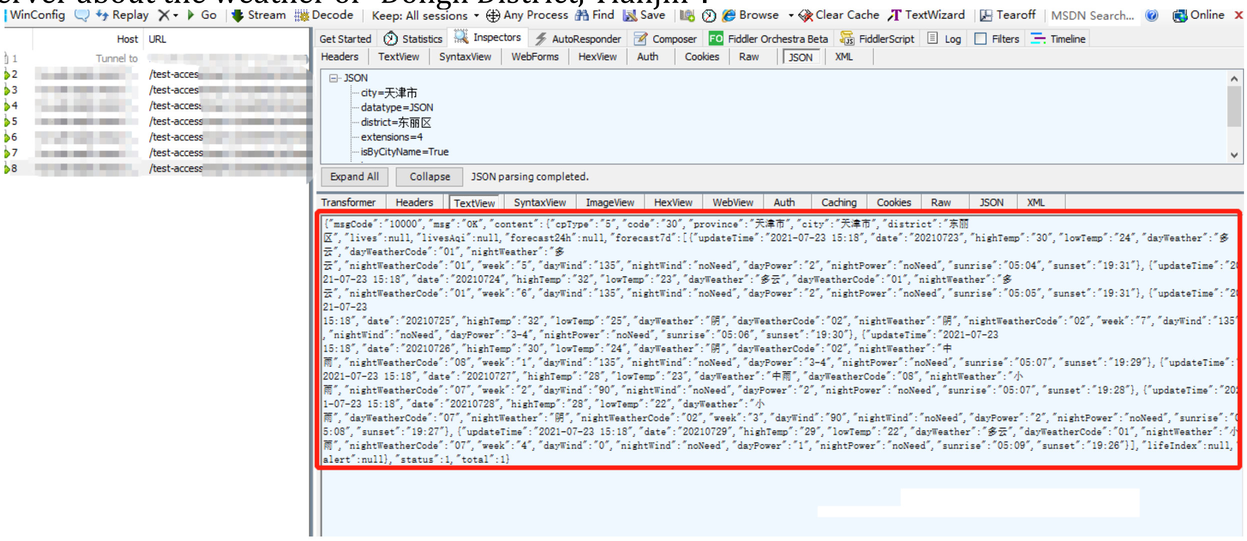
```
POST [redacted]
timestamp: 1627029669772
source: w37cD0
sign: 01C63EFFCF3FAAAB4C0A905147349DDB
language: zh-Hans
unit: c
Content-Type: application/json;charset=utf-8
Content-Length: 167
Host: [redacted]
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/4.2.2

{"city":"北京市","district":"东城区","extensions":"4",[redacted]":true,"lat":"39.904221049076796","lng":"116.40708241637125","datatype":"JSON","provider":"0"}
```

Modify the provincial, longitude and latitude information and resend

Figure 4: Fiddler changes packet parameters

Step 4: Get the response

Double-click the newly sent request, as shown in Figure 5, and get the correct response of the server about the weather of "Dongli District, Tianjin".


WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search... Online
Host URL
1 Tunnel to
2 /test-access
3 /test-access
4 /test-access
5 /test-access
6 /test-access
7 /test-access
8 /test-access
Get Started Statistics Inspectors AutoResponder Composer Fiddler Orchestra Beta FiddlerScript Log Filters Timeline
Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML
Expand All
Collapse
Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies Raw JSON XML

```
JSON
  city=天津市
  datatype=JSON
  district=东丽区
  extensions=4
  isByCityName=True
```

JSON parsing completed.

```
{"msgCode":"10000","msg":"OK","content":{"cpType":"5","code":"30","province":"天津市","city":"天津市","district":"东丽
区","lives":null,"livesAqi":null,"forecast24h":null,"forecast7d":[{"updateTime":"2021-07-23 15:18","date":"20210723","highTemp":"30","lowTemp":"24","dayWeather":"多
云","dayWeatherCode":"01","nightWeather":"多
云","nightWeatherCode":"01","week":"5","dayWind":"135","nightWind":"noNeed","dayPower":"2","nightPower":"noNeed","sunrise":"05:04","sunset":"19:31"},{"updateTime":"20
21-07-23 15:18","date":"20210724","highTemp":"32","lowTemp":"23","dayWeather":"多云","dayWeatherCode":"01","nightWeather":"多
云","nightWeatherCode":"01","week":"6","dayWind":"135","nightWind":"noNeed","dayPower":"2","nightPower":"noNeed","sunrise":"05:05","sunset":"19:31"},{"updateTime":"20
21-07-23
15:18","date":"20210725","highTemp":"32","lowTemp":"25","dayWeather":"阴","dayWeatherCode":"02","nightWeather":"阴","nightWeatherCode":"02","week":"7","dayWind":"135"
,"nightWind":"noNeed","dayPower":"3-4","nightPower":"noNeed","sunrise":"05:06","sunset":"19:30"},{"updateTime":"2021-07-23
15:18","date":"20210726","highTemp":"30","lowTemp":"24","dayWeather":"阴","dayWeatherCode":"02","nightWeather":"中
雨","nightWeatherCode":"08","week":"1","dayWind":"135","nightWind":"noNeed","dayPower":"3-4","nightPower":"noNeed","sunrise":"05:07","sunset":"19:29"},{"updateTime":"
2021-07-23 15:18","date":"20210727","highTemp":"28","lowTemp":"23","dayWeather":"中雨","dayWeatherCode":"08","nightWeather":"小
雨","nightWeatherCode":"07","week":"2","dayWind":"90","nightWind":"noNeed","dayPower":"2","nightPower":"noNeed","sunrise":"05:07","sunset":"19:28"},{"updateTime":"202
1-07-23 15:18","date":"20210728","highTemp":"28","lowTemp":"22","dayWeather":"小
雨","dayWeatherCode":"07","nightWeather":"阴","nightWeatherCode":"02","week":"3","dayWind":"90","nightWind":"noNeed","dayPower":"2","nightPower":"noNeed","sunrise":"0
5:08","sunset":"19:27"},{"updateTime":"2021-07-23 15:18","date":"20210729","highTemp":"29","lowTemp":"22","dayWeather":"多云","dayWeatherCode":"01","nightWeather":"小
雨","nightWeatherCode":"07","week":"4","dayWind":"0","nightWind":"noNeed","dayPower":"1","nightPower":"noNeed","sunrise":"05:09","sunset":"19:26"}],"lifeIndex":null,"
alert":null},"status":1,"total":1}
```

Figure 5: Server Response Result

6. Conclusion

The security problems brought by the Internet of vehicles cannot be underestimated. How to improve the security while providing better services is a topic worth exploring.Only on the basis of discovering problems and understanding the causes of problems can we better solve problems. Therefore, this paper studies the security testing technology of the IVI based on unilateral authentication bypass. While testing the security of unilateral identity authentication of vehicle entertainment system, it also understands some technical methods that will reduce its security, so as to provide a basis for preventing problems in the future.

References

[1] Wang Wenyang,Chen Zheng,Gao Xiran,Hu Ning,Zhang Dongwei: Vehicle entertainment system information security[J], Information Technology and Iformatization, (2018) No.12,p.106-107.

[2] Yu Mingming,Ning Yuqiao,Liu Tianyu,Guo Zhen: Research and analysis on information security of mobile APP in Internet of Vehicles[J], Auto Parts and Components, (2021) No.06,p.21-25.

[3] Lei Chao,Lin Cong: Remote user identity authentication[J], Journal of Sichuan Institute of Light Chemical Engineering,(2001)No.01,p.51-53.

[4] Liu Xinliang,Du Ruiying,Chen Jing,Wang Chiheng,Yao Shixiong,Chen Jiong: Security threats and defense methods for SSL/TLS session keys[J],Computer Engineering, Vol.43(2017)No.03,p.147-153.

[5] LiFeng,Chen Xin:Discussion on PKI system architecture based on LTE-V2X technology[J], Information Technology and Network Scurity, Vol.39(2020) No.07, p.41-47.

[6] Liu Hao,Zhang Ling,Zhang Jie,Wang Qian: Research on Vehicle Terminal Information Security Testing technology[J], Safety and Electromagnetic Compatibility, (2013) No.03,p.43-45.