# IVISTA

网 联 智 能 与 隐 私 安 全 专 项 测 评

编号：IVISTA-CIPS-SM-CSPS.CS-TP-A0-2023

# 网络与隐私安全
# 网络安全试验规程

Cybersecurity and Privacy Security

Cybersecurity Test Protocol

（2023 版）



中国汽车工程研究院股份有限公司 发布

# 目　次

# 网络安全试验规程

## 1 范围

本文件规定了网络与隐私安全测评中网络安全的试验方法。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 12572-2008 无线电发射设备参数通用要求和测量方法

GB/T 25069-2022 信息安全技术 术语

GB/T 37729-2019 信息技术 智能移动终端应用软件（App）技术要求

GB/T 38628-2020 信息安全技术 汽车电子系统网络安全指南

GB/T 38648-2020 信息安全技术 蓝牙安全指南

GB/T 40856-2021 车载信息交互系统信息安全技术要求及试验方法

GB/T 40857-2021 汽车网关信息安全技术要求及试验方法

GB/T 40861-2021 汽车信息安全通用技术要求

GB/T 41578-2022 电动汽车充电系统信息安全技术要求及试验方法

20214422-Q-339 汽车整车信息安全技术要求

20214423-Q-339 汽车软件升级通用技术要求

BD 110001-2015 北斗卫星导航术语

BD 410001-2015 北斗/全球卫星导航系统（GNSS）接收机数据自主交换格式

SJ/T 11421-2010 GNSS 测量型接收设备通用规范

IEEE 802.15 基于蓝牙的局域网标准

CSAE 252-2022 智能网联汽车车载端信息安全测试规程

## 3 术语和定义

以下术语和定义适用于本文件。

3.1

**射频 radio frequency；RF**

无线电频率，用于传输和接收无线信号。

3.2

**蓝牙 bluetooth**

一种无线通信技术，用于在短距离范围内连接设备，实现数据传输和通信。

3.3

**低功耗蓝牙 bluetooth low energy；BLE**

一种蓝牙通信技术，与经典蓝牙相比在保持同等通信范围时可显著降低功耗和成本。

3.4

**近场通讯 near field communication；NFC**

一种短距离无线通信技术，用于在设备之间进行数据传输和交换。

3.5

**射频钥匙 RF key**

使用射频技术的电子钥匙，可以通过无线信号与设备通信，用于解锁或控制车辆。

3.6

**NFC 钥匙 NFC key**

使用 NFC 技术的电子钥匙，可以通过近场通讯连接到设备或系统，用于解锁或控制车辆。

3.7

**全球导航卫星系统 global navigation satellite system；GNSS**

能在全球范围内提供导航服务的卫星导航系统。

3.8

**控车 App vehicle control application**

一种移动应用程序，利用无线通信技术（如蓝牙、Wi-Fi、移动网络等）与汽车通信，实现远程控制和管理汽车的各项功能，如执行启动或停止发动机、锁定或解锁车门、监控车辆位置和状态、调节车内温度等。

3.9

**重放攻击 replay attack**

通过记录通信会话，在某个时刻重放整个或部分会话的攻击方式。

3.10

**中继攻击 relay attack**

通过截获和中转两个合法通信实体之间的信息，来实现未授权的访问或其他恶意操作的攻击方式。

3.11

**篡改攻击 tampering attack**

通过捕获通信会话，修改会话中部分或全部数据内容，再次发送该会话内容的攻击方式。

3.12

**恶意程序 malicious program**

专门设计用来对计算机系统、网络或设备执行未经授权的、通常有害的操作的软件或脚本（如：木马程序、蠕虫病毒、勒索软件、间谍软件、广告软件、后门程序等）。恶意程序的目的包括但不限于窃取、加密或删除敏感数据；监控用户的活动；秘密访问或占用计算机系统资源；在受感染的设备上安装额外的恶意或潜在不需要的软件。

3.13

**车载诊断系统 on-board diagnostics；OBD**

车辆自诊断和报告能力系统。通过 OBD 接口，可以获取到车辆的各种运行状态信息，如引擎温度、转速、车速、故障代码等。

3.14

**安卓调试桥 android debug bridge；ADB**

允许开发者与连接的安卓设备或安卓虚拟设备进行通信的多功能命令行工具，属于安卓软件开发工具包，可为应用开发者提供设备管理接口，以执行安装和调试应用、访问设备上的文件系统、从设备上安装或卸载应用程序等操作。

3.15

**移动热点 wireless fidelity；Wi-Fi**

允许设备通过无线方式连接到互联网或局域网的无线网络技术。Wi-Fi 技术基于 IEEE 802.11 系列标准，通过无线电波在设备之间传输数据。

3.16

**DE-AUTH 攻击 deauthentication attack**

通过向 Wi-Fi 接入点或客户端发送伪造的去认证帧，迫使目标设备断开与 Wi-Fi 网络连接的攻击方式。

3.17

**钓鱼攻击 phishing attack**

通过伪装成可信的实体，欺骗用户以获取其敏感信息的网络攻击方式。

3.18

**全球移动通信系统 global system for mobile communications；GSM**

由欧洲电信标准组织制定的数字移动通信标准，是主要的蜂窝移动通信系统之一。

3.19

**伪基站 fake base station**

一种模拟真实基站的设备，通常用于无线通信的监听、干扰或攻击。

3.20

**模糊测试 fuzz testing**

一种自动化测试技术，用于发现软件或系统中的漏洞、错误或安全问题。

3.21

**软件升级 software update**

将某版本的软件通过升级包更新到新版本（包括更改软件的配置参数）的过程。

**注1：**“软件升级”也称“软件更新”。

**注2：**“软件升级”包含“在线升级”和“离线升级”。

[源：20214422-Q-339 汽车软件升级通用技术要求]。

3.22

**在线升级 over-the-air update；OTA update**

通过无线方式而不是使用电缆或其他本地连接方式将升级包传输到车辆的软件升级。

**注 1：**“在线升级”也称“远程升级”。

**注 2：**“本地连接方式”一般指通过车载诊断（OBD）接口、通用串行总线（USB）接口等进行的物理连接方式。

[源：20214422-Q-339 汽车软件升级通用技术要求]。

3.23

**离线升级 offline update**

除在线升级以外的软件升级。

[源：20214423-Q-339 汽车软件升级通用技术要求]。

3.24

**CAERI 车联网攻防靶场 CAERI internet of vehicles attack and defense range**

专为车联网环境设计的测试和评估平台，旨在模拟各种网络攻击和防御场景，以评估车联网系统和技术的安全性。可为研究人员、开发人员和安全专家在不影响真实世界的情况下，测试和验证车联网技术的安全性能提供安全的实验环境。

## 4 试验要求

### 4.1 试验场地及试验环境

#### 4.1.1 试验场地要求

a）试验应选择宽敞平坦的开放性测试场地或整车屏蔽室；

b）涉及无线通信等相关试验应选取整车屏蔽室作为试验场地，避免无线信号的干扰和反射；

c）开放性测试场地两侧与静止目标车前方 30 米内无任何车辆、障碍物或其他影响试验的物体。

#### 4.1.2 试验环境要求

a）在测试过程中，避免其他无线设备的干扰，确保测试环境的纯净性；

b）屏蔽室环境下，测试人员需将手机、平板等对外通信设备置于屏蔽室外；

c）试验车辆离线升级前，对升级数据进行完整备份，以防止升级过程中的数据丢失或损坏。

### 4.2 试验设备要求

a）检查测试仪器的工作状态和电源供应，确保其正常运行；

b）根据测试需要，对测试仪器进行校准和校验，以消除仪器误差对测试结果的影响；

c）确保测试仪器的固定和安装稳固，避免在测试过程中发生不必要的移动或震动；

d）部署网络环境时，采用安全配置，包括防火墙设置、网络隔离等，以防范潜在的网络攻击。

### 4.3 车辆准备

#### 4.3.1 车辆状态确认

a）试验车辆应为新车，行驶里程不高于 5000 公里；

b）车辆抵达试验场地后，检查车辆状态是否完好，确认零部件完整、整车外观无明显损坏、状态指示灯正常、整车上电及自检功能正常、试验相关系统功能正常。若有异常则记录，若异常状态与试验相关，则应对其修复或更换车辆；

c）对于燃油车，确保燃油量达到油箱容积的 50% 以上；对于可外接充电的新能源车辆，电量不低于最大容量的 50%。

#### 4.3.2 功能检查

试验车辆功能检查包含但不限于如下方面：

a）试验车辆无线通信设备，如车载通信模块、无线网卡、Wi-Fi热点、蓝牙通信等功能正常；

b）试验车辆射频钥匙、NFC钥匙、蓝牙钥匙功能正常；

c）试验车辆导航定位功能正常；

d）试验车辆控车App功能正常；

e）试验车辆各接口功能正常；

f）试验车辆软件升级功能正常，满足进行升级的先决条件（例如电量、油量等)。

### 4.4 试验过程及结果记录

a）试验开始前，对车辆信息进行拍照记录，包括在车左前方 45° 对整车进行拍照和车辆铭牌进行拍照；

b）试验车辆安装音视频拍摄设备，拍照记录车辆状态，应满足如下要求：

——应记录试验车辆车门状态；

——应记录试验车辆仪表盘、中控台显示信息及系统提示；

——应记录试验充电桩与车辆充电口的信息（若有）。

## 5 试验方法

网络安全试验项目包括数字钥匙安全试验、导航定位安全试验、远程控车安全试验、车端接口安全试验、网络通信安全试验及极限攻防安全试验 6 个部分。具体试验方法见附录 A-附录 F。

# 附录 A

# 数字钥匙安全试验方法

## A.1 射频钥匙重放攻击试验

该试验用于评价车辆在锁车状态下抵抗射频钥匙信号重放攻击的能力。

a）试验方法：

1）车辆接收响应范围内，使用射频钥匙测试套件录制并重放射频钥匙解锁信号，观察车辆是否被解锁，记录试验结果为结果1（若车辆未被解锁，则进行步骤2；若车辆被解锁，则射频钥匙重放攻击试验结束）；

2）车辆接收响应范围外，使用射频钥匙测试套件录制并重放射频钥匙解锁信号，观察车辆是否被解锁，记录试验结果为结果2。

b）结果记录：

观察并记录车辆响应，并填写下表：

表A.1 射频钥匙重放攻击试验结果记录表

| 结果记录 | 结果指标 |
|---|---|
| 结果1：车辆是否被解锁 | □是 □否 □不适用 |
| 结果2：车辆是否被解锁 | □是 □否 □不适用 |

## A.2 蓝牙钥匙重放攻击试验

该试验用于评价车辆在锁车状态下抵抗蓝牙钥匙信号重放攻击的能力。

a）试验方法：

使用蓝牙钥匙测试套件重放蓝牙钥匙解锁信号，观察车辆是否被解锁。

b）结果记录：

观察并记录车辆响应，并填写下表：

表A.2 蓝牙钥匙重放攻击试验结果记录表

| 结果记录 | 结果指标 |
|---|---|
| 车辆是否被解锁 | □是 □否 □不适用 |

## A.3 蓝牙钥匙中继攻击试验

该试验用于评价车辆在锁车状态下抵抗蓝牙钥匙信号中继攻击的能力。

a）试验方法：

使用蓝牙钥匙测试套件中继蓝牙钥匙解锁信号，观察车辆是否被解锁。

b）结果记录：

观察并记录车辆响应，并填写下表：

**表A.3 蓝牙钥匙中继攻击试验结果记录表**

| 结果记录 | 结果指标 |
|---|---|
| 车辆是否被解锁 | □是 □否 □不适用 |

## A.4 NFC 钥匙中继攻击试验

该试验用于评价车辆在锁车状态下抵抗NFC钥匙信号中继攻击的能力。

a）试验方法：

1）使用NFC钥匙测试套件中继NFC钥匙（实体卡片NFC钥匙）解锁信号，观察车辆是否被解锁，记录试验结果为结果1。

2）使用NFC钥匙测试套件中继NFC钥匙（智能设备NFC钥匙）解锁信号，观察车辆是否被解锁，记录试验结果为结果2。

b）结果记录：

观察并记录车辆响应，并填写下表：

**表A.4 NFC钥匙中继攻击试验结果记录表**

| 结果记录 | 结果指标 |
|---|---|
| 结果1：车辆是否被解锁 | □是 □否 □不适用 |
| 结果2：车辆是否被解锁 | □是 □否 □不适用 |

# 附录 B

# 导航定位安全试验方法

## B.1 GNSS 信号伪造试验

该试验用于评价车辆抵抗虚假的GNSS信号避免车辆定位错误或者受到误导的能力。

a）试验方法：

1）打开车辆无线通信（蜂窝网络、蓝牙通信、Wi-Fi通信），使用GNSS测试套件伪造GNSS信号对车辆进行GNSS欺骗，观察车辆定位服务是否发生变化（若定位服务发生变化，则GNSS信号伪造测试结束；若定位服务未发生变化，则进行步骤2），记录试验结果为结果1；

2）关闭车辆无线通信（蜂窝网络、蓝牙通信、Wi-Fi通信），使用GNSS测试套件伪造GNSS信号对车辆进行GNSS欺骗，观察车辆定位服务是否发生变化，记录试验结果为结果2。

b）结果记录：

观察并记录车辆响应，并填写下表：

表B.1 GNSS信号伪造试验结果记录表

| 结果记录 | 结果指标 |
|---|---|
| 结果1：车辆定位服务是否定位到指定位置 | □是 □否 □不适用 |
| 结果2：车辆定位服务是否定位到指定位置 | □是 □否 □不适用 |

## B.2 GNSS 信号干扰试验

该试验用于评价车辆使用GNSS系统进行定位时，受到外部干扰导致信号质量下降或定位精度受影响的情况。

a）试验方法：

1）打开车辆无线通信（蜂窝网络、蓝牙通信、Wi-Fi通信），使用GNSS测试套件对车辆进行GNSS干扰，观察车辆定位服务是否无法正确定位（若定位服务未正确定位，则GNSS信号干扰测试结束；若定位服务正确定位，则进行步骤2），记录试验结果为结果1；

2）关闭车辆无线通信（蜂窝网络、蓝牙通信、Wi-Fi通信），使用GNSS测试套件对车辆进行GNSS干扰，观察车辆定位服务是否无法正确定位，记录试验结果为结果2。

b）结果记录：

观察并记录车辆响应，并填写下表：

表B.2 GNSS信号干扰试验结果记录表

| 结果记录 | 结果指标 |
| --- | --- |
| 结果1：车辆定位服务是否无法正确定位 | □是 □否 □不适用 |
| 结果2：车辆定位服务是否无法正确定位 | □是 □否 □不适用 |

# 附录 C

# 远程控车安全试验方法

## C.1 控车 App 安全扫描试验

该试验用于测试控车App基线配置是否安全，是否存在安全漏洞。

a）试验方法：

1）记录控车App软件包版本号；

2）安全漏洞扫描。将控车App软件包导入App漏扫工具，开启基线扫描和全漏洞扫描模式。检查控车App的安全配置，如HTTPS使用情况、证书验证、数据加密、安全加固等；检查App是否存在安全漏洞（低危漏洞≤5，且无中高危漏洞为安全，反之则为不安全）。

b）结果记录：

观察并记录车辆响应，并填写下表：

表C.1 控车App安全扫描试验结果记录表

| 结果记录 | 结果指标 |
| --- | --- |
| App基线扫描是否安全 | □是 □否 □不适用 |
| App漏洞扫描是否安全 | □是 □否 □不适用 |

## C.2 控车 App 通信安全性试验

该试验用于测试控车App是否使用安全的传输协议进行通信。

a）试验方法：

1）在标准测试机或标准模拟器安装对应测试车辆的控车App，保证测试设备与测试车辆能够进行通信；

2）开启ADB调试，使用测试电脑接入ADB，运行数据抓包工具；

3）运行控车App，触发远程控车功能（如：远程解锁、鸣笛、亮灯等），使用数据抓包工具抓取控车通信数据包；

4）导出捕获的通信数据包，使用数据分析工具查看通信是否使用安全的传输协议（使用HTTPS协议且经过SSL/TLS加密处理，TLS版本大于等于1.2；或使用IPsec协议）。

b）结果记录：

观察并记录车辆响应，并填写下表：

表C.2 控车APP通信安全性试验结果记录表

| 结果记录 | 结果指标 |
| --- | --- |
| 是否使用安全的传输协议 | □是 □否 □不适用 |

### C.3 App 控车指令重放攻击试验

该试验用于评价车辆在锁车状态下抵抗App控车信号重放攻击的能力。

a）试验方法：

1）在标准测试机或标准模拟器安装对应测试车辆的控车App，保证测试设备与测试车辆能够进行通信；

2）触发远程控车功能（如：远程解锁、鸣笛、亮灯等），使用中间人工具进行数据代理，抓取正常流量；使用中间人工具再次发送截取到的控车指令数据包，进行指令重放攻击，观察车辆是是否执行控制操作。

b）结果记录：

观察并记录车辆响应，并填写下表：

表C.3 APP控车指令重放攻击试验结果记录表

| 结果记录 | 结果指标 |
| --- | --- |
| 车辆是否执行控制操作 | □是 □否 □不适用 |

### C.4 App 控车指令篡改攻击试验

该试验用于评价车辆在锁车状态下抵抗App控车信号被篡改的能力。

a）试验方法：

1）在标准测试机或标准模拟器安装对应测试车辆的控车App，保证测试设备与测试车辆能够进行通信；

2）触发远程控车功能（如：远程解锁、鸣笛、亮灯等），使用中间人工具进行数据代理，抓取正常流量；使用中间人工具篡改截取的控车指令数据包并重新发送，进行指令篡改攻击，观察车辆是是否执行控制操作。

b）结果记录：

观察并记录车辆响应，并填写下表：

表C.4 APP控车指令篡改攻击试验结果记录表

| 结果记录 | 结果指标 |
| --- | --- |
| 车辆是否执行控制操作 | □是 □否 □不适用 |

# 附录 D

# 车端接口安全试验方法

## D.1 USB 接口试验

### D.1.1 USB 接口访问控制试验

该试验用于评估车辆 USB 接口的文件识别机制，确保 USB 接口只能读取特定格式的文件。

a）试验方法：

1）检查车机系统中的应用情况，查看车机实况可识别文件类型，查看车辆使用说明中声明文件识别类型，合并检查结果列出文件识别清单；

2）根据步骤 1）制作包含以上文件类型及其他文件类型的 USB 接口检测设备；

3）使用 USB 接口检测设备接入车辆 USB 接口，使用车机中具备文件管理功能的 App，查看车机是否仅能识别清单允许格式的文件。

b）结果记录：

观察并记录车机对文件格式的识别结果，并填写下表：

**表 D.1.1 USB 接口访问控制试验结果记录表**

| 结果记录 | 结果指标 |
|---|---|
| 是否仅能识别清单允许格式的文件 | □是　　□否　　□不适用 |

### D.1.2 USB 接口防病毒试验

该试验用于评估车辆 USB 接口的防病毒机制，确保 USB 接口不会被病毒影响。

a）试验方法：

使用硬件测试套件接入车辆 USB 接口，观察车机是否自动执行硬件测试套件中所携带的恶意测试程序；通过文件管理器触发硬件测试套件中所携带的恶意测试程序，观察车机对病毒反应情况。

b）结果记录：

观察并记录车机对病毒的反应情况，并填写下表：

**表 D.1.2 USB 防病毒试验结果记录表**

| 结果记录 | 结果指标 |
|---|---|
| 是否运行恶意程序 | □是　　□否　　□不适用 |

### D.1.3 ADB 调试安全检查试验

该试验用于评估车辆 USB 接口是否具备调试功能，确保 USB 接口调试功能关闭或具有访问控制。

a）试验方法：

1）使用标准测试电脑接入车辆 USB 接口，在标准测试电脑中尝试连接 ADB，观察 ADB 是否能够连接成功（若成功接入 ADB 调试，则进行步骤 2；若未能接入 ADB 调试，则 ADB 调试安全检查试验结束）；

2）查看当前用户权限，或使用 su 命令查看 ADB 调试是否能够启用 root 权限。

b）结果记录：

观察并记录车机 ADB 接口的测试结果，并填写下表：

**表 D.1.3 ADB 调试安全试验结果记录表**

| 结果记录 | 结果指标 |
|---|---|
| 是否可接入ADB调试 | □是 □否 □不适用 |
| ADB调试是否启用root权限 | □是 □否 □不适用 |

### D.2 OBD 接口访问控制试验

该试验用于评估针对高风险指令（如篡改、复位等），OBD 接口是否具备访问控制机制，以确保非授权用户接入车辆的诊断系统后，无法进行数据操纵或获取重要数据。

a）试验方法：

使用标准测试电脑和总线测试套件连接车辆 OBD 接口，使用标准测试电脑向车内总线发送需要访问权限的 UDS 诊断请求，观察车辆响应结果，分析访问控制机制是否有效。

b）结果记录：

观察并记录车机 OBD 接口的测试结果，并填写下表：

**表 D.2 OBD 接口试验结果记录表**

| 结果记录 | 结果指标 |
|---|---|
| 访问控制机制是否有效 | □是 □否 □不适用 |

### D.3 充电接口试验

### D.3.1 直流充电接口模糊攻击试验

该试验用于评价车辆在充电过程中，直流充电接口抵抗模糊攻击的能力。

a）试验方法：

a）试验方法：

1）将标准测试电脑和总线测试套件接入车辆直流充电口，使车辆接入直流充电桩开始充电；

2）使用标准测试电脑和总线测试套件对充电接口进行模糊攻击，时间为 15 分钟，观察车辆是否出现异常响应或停止充电的情况，记录试验结果。

b）结果记录：

观察并记录充电过程中车辆的充电状态信息，并填写下表：

**表 D.3.1 直流充电过程 CAN 攻击试验结果记录表**

| 结果记录 | 结果指标 |
| --- | --- |
| 车辆充电状态是否受到影响 | □是 □否 □不适用 |

### D.3.2 直流充电口的 CAN 隔离试验

该试验用于评估车辆在充电过程中对 CAN 网络的隔离措施，确保车辆不响应非充电相关 CAN 消息。

a）试验方法：

使用标准测试电脑和总线测试套件接入车辆的充电接口，通过充电口接入发送非充电相关的 CAN 消息到车辆内部网络，查看车辆是否响应非充电相关的 CAN 消息。

b）结果记录：

观察并记录车辆对非充电相关的 CAN 消息的响应情况，并填写下表：

**表 D.3.2 直流充电口的 CAN 隔离试验结果记录表**

| 结果记录 | 结果指标 |
| --- | --- |
| 是否能响应非充电相关的CAN消息 | □是 □否 □不适用 |

## D.4 远程连接服务试验

该试验用于试验车辆是否存在未授权的远程连接服务。

a）试验方法：

1）使用标准测试电脑开启Wi-Fi热点，车辆连接该Wi-Fi热点，使用标准测试电脑对车辆进行网络端口扫描，记录端口扫描结果，查看车辆是否存在未授权的远程连接服务；

2）开启车辆热点功能（若有），并使用标准测试电脑连接至车辆热点，使用标准测试电脑对车辆进行网络端口扫描，记录端口扫描结果，查看车辆是否存在未授权的远程连接服务。

b）结果记录：

观察并记录端口扫描结果，并填写下表：

表 D.4 远程连接试验结果记录表

| 结果记录 | 结果指标 |
| --- | --- |
| 车辆是否存在未授权的远程连接服务 | □是 □否 □不适用 |

# 附录 E

# 网络通信安全试验方法

## E.1 Wi-Fi 热点破解攻击试验

该试验用于评价车辆在热点开启状态下抵抗Wi-Fi热点密码暴力破解的能力。

a）试验方法：

1）恢复车辆出厂设置，检查车辆Wi-Fi热点默认密码是否符合强度要求，记录试验结果为结果1；

2）修改车辆Wi-Fi热点密码为弱密码（仅包含数字或字母的口令），观察车辆是否对密码强度有校核并进行提示，记录试验结果为结果2；

3）修改车辆Wi-Fi热点密码为弱密码（仅包含数字或字母的口令），观察车辆是否会限制密码修改，记录试验结果为结果3。

b）结果记录：

观察并记录车辆响应，并填写下表：

表E.1 Wi-Fi热点破解试验结果记录表

| 结果记录 | 结果指标 |
|---|---|
| 结果1：车辆热点默认密码是否是8位以上数字、大小写字母、特殊符号两种以上的组合 | □是 □否 □不适用 |
| 结果2：车辆修改密码是否会有强度提示 | □是 □否 □不适用 |
| 结果3：车辆修改密码是否会强制要求 | □是 □否 □不适用 |

## E.2 Wi-Fi 断连攻击试验

该试验用于评价车辆在Wi-Fi热点开启状态下抵抗DE-AUTH攻击的能力。

a）试验方法：

默认状态下开启车辆热点，使用Wi-Fi测试套件对车辆热点进行DE-AUTH攻击，观察测试设备与车辆热点是否断开连接。

b）结果记录：

观察并记录车辆响应，并填写下表：

表E.2 Wi-Fi断连攻击试验结果记录表

| 结果记录 | 结果指标 |
| --- | --- |
| 车辆热点是否与测试设备断开连接 | □是 □否 □不适用 |

## E.3 恶意钓鱼 Wi-Fi 攻击试验

该试验用于评价车辆在Wi-Fi连接状态下抵抗恶意钓鱼Wi-Fi攻击的能力。

a）试验方法：

使用Wi-Fi测试套件创建钓鱼Wi-Fi（与测试主机热点具备相同SSID，无密码），观察车辆开启Wi-Fi是否自动连接到恶意钓鱼Wi-Fi。

b）结果记录：

观察并记录车辆响应，并填写下表：

表E.3 恶意钓鱼Wi-Fi试验结果记录表

| 结果记录 | 结果指标 |
| --- | --- |
| 车辆是否自动连接到恶意钓鱼Wi-Fi | □是 □否 □不适用 |

## E.4 Wi-Fi 协议模糊攻击试验

该试验用于评价车辆Wi-Fi功能抵抗模糊攻击的能力。

a）试验方法：

默认状态下开启车辆热点，使用Wi-Fi测试套件对车辆热点进行协议模糊攻击，时间为15分钟，观察车辆Wi-Fi是否正常工作。

b）结果记录：

观察并记录车辆响应，并填写下表：

表E.4 Wi-Fi协议模糊攻击试验结果记录表

| 结果记录 | 结果指标 |
| --- | --- |
| 车辆Wi-Fi是否正常工作 | □是 □否 □不适用 |

## E.5 蓝牙通信信息窃取攻击试验

该试验用于评价车辆低功耗蓝牙通信抵抗信息窃取的能力。

a）试验方法：

使用蓝牙测试套件捕获车辆低功耗蓝牙配对通信数据包，分析通信数据是否具备安全配对流程。

b）结果记录：

观察并记录车辆响应，并填写下表：

表E.5 蓝牙通信信息窃取攻击试验结果记录表

| 结果记录 | 结果指标 |
| --- | --- |
| 通信数据是否具备安全配对流程 | □是 □否 □不适用 |

## E.6 蓝牙协议模糊攻击试验

该试验用于评价车辆低功耗蓝牙与经典蓝牙抵抗模糊攻击的能力。

a）试验方法：

1）使用蓝牙测试套件对试验车辆低功耗蓝牙进行协议模糊攻击，时间为15分钟，观察车辆低功耗蓝牙是否正常工作，记录试验结果。

2）使用蓝牙测试套件对试验车辆经典蓝牙进行协议模糊攻击，时间为15分钟，观察车辆经典蓝牙是否正常工作，记录试验结果。

b）结果记录：

观察并记录车辆响应，并填写下表：

表E.6 蓝牙协议模糊攻击试验结果记录表

| 结果记录 | 结果指标 |
| --- | --- |
| 低功耗蓝牙是否正常工作 | □是 □否 □不适用 |
| 经典蓝牙是否正常工作 | □是 □否 □不适用 |

## E.7 GSM 网络劫持攻击试验

该试验用于评价车辆抵抗GSM网络劫持攻击的能力。

a）试验方法：

1）将试验车辆置于屏蔽室内，使用蜂窝测试套件搭建伪基站，触发车辆对外通信流程，观察车辆是否接入伪基站，并记录结果为结果 1 。（若车辆接入伪基站，则执行步骤 2 ；若车辆未接入伪基站，则GSM网络劫持攻击试验结束。）

2）观察试验车辆对外通信功能是否正常，并记录测试结果为结果 2。

b）结果记录：

观察并记录车辆响应，并填写下表：

表E.7 GSM网络劫持试验结果记录表

| 结果记录 | 结果指标 |
| --- | --- |
| 结果1：车辆是否接入伪基站 | □是 □否 □不适用 |
| 结果2：车辆对外通信功能是否正常 | □是 □否 □不适用 |

## E.8 升级刷写设备认证试验

该试验用于评估试验车辆OBD接口刷写过程中的身份认证机制,确保只有授权设备和操作者能够进行刷写操作。

a）试验方法：

使用刷写测试套件模拟车辆刷写过程，对试验车辆进行刷写，观察车辆是否返回肯定响应。

b）结果记录：

观察并记录车辆响应，并填写下表：

表E.8 升级刷写设备认证试验结果记录表

| 结果记录 | 结果指标 |
| --- | --- |
| 车辆是否返回肯定响应 | □是 □否 □不适用 |

# 附录 F

# 极限攻防安全试验方法

## F.1 极限攻防安全试验

该试验用于检测车辆在极限攻防测试下的安全程度。

a）试验方法：

1）生产制造商根据自身情况提供表 F.1 中输入项目内容；

**表F.1 极限攻防安全输入项目清单**

| 输入项目 | 输入内容 |
| --- | --- |
| 车载信息娱乐系统/IVI | 1、ADB/Telnet/SSH等远程调试接口<br>2、零部件及主要外部接口说明 |
| 车载通信系统/TBOX | |
| 车载网关 | |
| 自动驾驶域控制器 | |

注：外部接口包括本零部件与其他零部件通信的 CAN、以太网、LIN 等通信接口定义，以及供电和唤醒引脚定义。

2）试验车辆接入 CAERI 汽车网络安全攻防靶场，攻击系统使用 CVE、CNVD、NVDB 等公开的漏洞数据以及中国汽研漏洞库中的漏洞数据，对车辆进行攻击仿真模拟，并记录车辆测试情况；

3）试验车辆接入 CAERI 汽车网络安全攻防靶场，中国汽研邀请专业团队通过实战化的攻击手法，结合生产制造商针对表 F.1 反馈情况，对车辆进行自由渗透，测试时间持续 10 天。测试过程中，靶场管理团队对各测试团队加以控制和引导，覆盖常见车辆渗透测试攻击面和攻击路径，并记录车辆测试情况。

b）结果记录：

观察并记录漏洞数量，并填写下表：

**表F.2 极限攻防安全试验结果记录表**

| 结果记录 | 结果指标（个） |
| --- | --- |
| 低危漏洞数量 | |
| 中危漏洞数量 | |
| 高危漏洞数量 | |
| 严重漏洞数量 | |