

IVISTA

网联智能与隐私安全专项测评

编号: IVISTA-XXXX-XX-XXXX.XX-XX-XX-XXXX

网络与隐私安全 网络安全试验规程

Cybersecurity and Privacy Security

Cybersecurity Test Protocol

(2023 版修订版)

中国汽车工程研究院股份有限公司 发布

目 次

1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
4 试验要求.....	4
5 试验方法.....	5
附录 A 数字钥匙安全试验方法.....	6
附录 B 导航定位安全试验方法.....	8
附录 C 远程控车安全试验方法.....	9
附录 D 车端接口安全试验方法.....	12
附录 E 网络通信安全试验方法.....	15
附录 F 极限攻防安全试验方法.....	19

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 44495-2024 汽车整车信息安全技术要求

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 40861-2021 汽车信息安全通用技术要求

SJ/T 11421-2010 GNSS 测量型接收设备通用规范

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

一种采用射频方式在近距离使用电子信息设备交换信息的无线接口技术。

[源：GB/T 38648-2020，3.1]

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，以便某个时刻重放整个或部分会话的主动攻击方式。

[源：GB/T 25069-2022，有修改]

3.10

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。

3.11

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。

3.12

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。

3.13

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。

3.14

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。

3.15

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。

3.16

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。

3.17

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。

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。

4.2 试验设备要求

- a) 检查测试仪器的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。

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) 试验完成后，通过拍照或录像的方式记录车辆状态，包括但不限于试验车辆车门状态、仪表盘、中控台显示信息及系统提示等。

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

结果指标	结果记录		
结果1: 车辆是否被解锁	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
结果2: 车辆是否被解锁	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 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

结果指标	结果记录		
车辆是否被解锁	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用

A.3 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

结果指标	结果记录		
结果1: 车辆是否被解锁	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
结果2: 车辆是否被解锁	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 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信号以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。观察车辆定位位置是否准确，记录试验结果为结果1。若车辆定位位置准确，则继续进行步骤2；若车辆定位位置不准确，则GNSS信号伪造试验结束；

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。观察车辆定位位置是否准确，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

结果指标	结果记录		
结果1: 车辆定位位置是否准确	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
结果2: 车辆定位位置是否准确	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用

附录 C

远程控车安全试验方法

C.1 控车 App 加固安全性试验

该试验用于测试控车App是否采取有效的安全加固措施，以防止逆向分析、动态调试和代码篡改等。

a) 试验方法：

1) 控车App加壳：使用查壳工具（如ApkScan、PKID、DexExtractor等）对控车App软件包进行分析，检查是否包含第三方加固壳（如腾讯御安全、梆梆加固、360加固等）；

若查壳工具识别到加壳特征，则记录加固类型及版本。若未识别到加壳特征，则通过反编译工具（如Jadx、Ghidra等）尝试解析代码，观察是否因加壳导致反编译失败或代码结构异常。

2) 控车App代码混淆：使用反编译工具（如Jadx、JEB等）分析App代码结构，检查类名、方法名、变量名是否被替换为无意义字符串（如a、b、c等）、检查代码逻辑中是否包含冗余指令或控制流混淆（如虚假分支、平坦化处理等）。

3) 控车App安全机制绕过：在标准测试机上安装Xposed框架及常见Hook模块（如JustTrustMe、SSLUnpinning等），尝试对控车App进行动态代码注入，观察控车App是否触发安全检测（如崩溃、弹窗警告或功能限制等）。

若App无安全检测机制，则不再进行绕过检测；若存在安全检测机制，则使用Frida工具注入控车App进程，尝试Hook关键函数（如加密算法、身份验证逻辑等），记录是否成功绕过检测。

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加固分析试验结果记录表

结果指标	结果记录				
控车App是否具备加固壳	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用		
控车App是否具备代码混淆	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用		
控车App安全机制绕过	安全检测机制		绕过检测		<input type="checkbox"/> 不适用
	<input type="checkbox"/> 具备	<input type="checkbox"/> 不具备	<input type="checkbox"/> 绕过成功	<input type="checkbox"/> 绕过失败	

C.2 控车 App 漏洞扫描试验

该试验用于测试控车App是否存在安全漏洞。

a) 试验方法:

将控车App软件包导入App漏扫工具，开启全漏洞扫描模式。检查App是否存在安全漏洞，记录安全漏洞类型及数量。

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漏洞扫描试验结果记录表

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	

C.3 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（如使用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协议等）。

b) 结果记录:

观察并记录车辆响应，并填写下表:

表C.3 控车APP通信安全性试验结果记录表

结果指标	结果记录
是否使用安全的传输协议	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不适用

C.4 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控车指令重放攻击试验结果记录表

结果指标	结果记录		
车辆是否执行控制操作	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用

C.5 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.5 APP控车指令篡改攻击试验结果记录表

结果指标	结果记录		
车辆是否执行控制操作	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 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，查看车机实际可识别文件类型，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

结果指标	结果记录		
是否仅能识别清单允许格式的文件	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 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：

1) 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；

2) 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

结果指标	结果记录
是否运行恶意程序	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 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

结果指标	结果记录
是否可接入ADB调试	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不适用
ADB调试是否启用root权限	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 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（如写数据、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，如写数据、复位等；再模拟车辆刷写过程，对试验车辆进行刷写，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

结果指标	结果记录
访问控制机制是否有效	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不适用

D.3 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), 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.3 远程连接试验结果记录表

结果指标	结果记录		
车辆是否存在未授权的远程连接服务	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 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(8位以上数字、大小写字母、特殊符号两种以上的组合), 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

结果指标	结果记录		
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	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
结果2: 车辆修改密码是否会有强度提示	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
结果3: 车辆修改密码是否会强制要求	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 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

结果指标	结果记录
车辆热点是否与测试设备断开连接	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 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

结果指标	结果记录
车辆是否自动连接到恶意钓鱼Wi-Fi	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 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

结果指标	结果记录
车辆Wi-Fi是否正常工作	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 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

结果指标	结果记录		
通信数据是否具备安全配对流程	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 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

结果指标	结果记录		
低功耗蓝牙是否正常工作	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
经典蓝牙是否正常工作	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 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	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
结果2：车辆对外通信功能是否正常	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用

征求意见稿

附录 F

极限攻防安全试验方法

F.1 控车 App 深度对抗试验

本试验旨在测试Android版控车App在面对黑客时，是否具备足够强度的加固手段，以防止黑客进一步发现安全问题。以及，当加固手段不够完善时，控车App蓝牙控车功能防护机制是否完善。

a) 试验方法：

1) 参照情报库中的对抗手段，对控车App加固机制进行手动分析，针对加固手段编写脚本，尝试对App进行脱壳、Frida/Xposed检测对抗、SSL Pinning检测对抗。若步骤1)无法绕过，则控车App深度对抗试验结束。

2) 若步骤1)能够绕过加固，则对手机的控车逻辑进行深度分析，针对身份认证、通信内容、权限控制等项目进行分析。

b) 结果记录：

表F.1 控车App深度对抗试验结果记录表

结果指标	结果记录		
是否能对控车App进行脱壳	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
是否能绕过Frida/Xposed检测	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
是否能绕过SSL Pinning检测	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
是否存在身份认证机制	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
是否能够绕过身份认证机制	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
是否包含通信数据校验	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
是否能还原校验字段的算法	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
是否存在权限控制	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
是否能绕过权限控制	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
未授权用户能否构造数据包并解锁车辆	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用

F.2 车内网络攻防试验

本试验将尝试对车辆进行拆解，寻找并接入TBOX/IVI/智能驾驶域控等核心控制器的接口，对零部件以及车辆内部通信进行深度测试，检查攻击链条上各环节是否安全。

a) 试验方法：

1) 拆解车辆并寻找IVI/TBOX/智驾域控制器，识别控制器的以太网接口，若发现以太网接口则接入后尝试对以太网通信进行嗅探。若步骤1)未发现相关接口，则车内网络攻防抗试验结束。

2) 根据嗅探到的IP地址信息，尝试接入车内以太网，对相应的零部件进行端口及服务扫描，识别已知服务，并使用漏洞库中的漏洞PoC，检测对应服务是否存在已知漏洞，若存在漏洞则按照漏洞库中的漏洞评级记录漏洞数量。

3) 若零部件存在ADB、Telnet、SSH等远程调试接口，则进行密码爆破及接入尝试。

4) 若取得零部件接入权限，则对程序及通信协议进行逆向分析，针对可能的操作系统提权、车内网络通信、车外通信接口等问题进行测试。

b) 结果记录：

表F.2 车内网络攻防试验结果记录表

结果指标	结果记录
能否识别以太网接口，且能够完成通信嗅探	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不适用
识别出的已知高危、严重漏洞数（个）	
识别出的已知中危漏洞数（个）	
识别出的已知低危漏洞数（个）	
能够获取调试接口权限的零部件数量（个）	
通过调试接口能够获取到system/root权限的零部件数量（个）	
能够受控发送以太网/CAN通信，以控制车辆解锁或车身动作的零部件数量（个）	
是否能够通过Wi-Fi/蓝牙控制车辆解锁或车身动作	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不适用

注：控制车身动作指能够控制转向、灯光、刹车、油门、挡位等涉及驾驶安全的操作。