ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 105-2022

移动终端控车应用软件信息安全

Testing specification for car control mobile application security

2022-11-02 发布　　2022-11-03 实施

吉林省汽车电子协会　发 布

目　　次

前　言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国第一汽车集团有限公司智能网联开发院、启明信息技术股份有限公司联合提出。

本文件由吉林省汽车电子协会归口。

本文件由吉林省汽车电子协会组织实施。

本文件主要起草单位：启明信息技术股份有限公司、中国第一汽车集团有限公司智能网联开发院。

本文件主要起草人：蒋澈、刘磊、宋迎亮、张鸿彪、魏利、徐焕、曾宪宇、王鹏、郭彧、尤涛、孙琦、禹晶晶、陈明。

本文件参与起草单位：吉林大学汽车仿真与控制国家重点实验室、中国汽车技术研究中心有限公司、中国汽车工程研究院股份有限公司、三六零数字安全科技集团有限公司、联通智网科技股份有限公司、一汽解放汽车有限公司商用车开发院、一汽-大众汽车有限公司、沙龙机甲科技有限公司、中电信数智科技有限公司长春分公司、中电福富信息科技有限公司。

本文件参与起草人：李杰、李宝田、全代勇、姚越航、田雪、刘书勇、高德志、王博、王思涵、高深、李新坚。

本文件审查人：杨彦鼎（东风汽车集团有限公司技术中心）、夏国强（中国汽车工程研究院股份有限公司）、马文峰（一汽奔腾轿车有限公司）、马喜来（一汽解放汽车有限公司）、占锐（东风汽车集团有限公司技术中心）、孔晓霜（中国第一汽车集团有限公司创新技术研究院）。

本文件为首次发布。

引　言

为了确保移动终端控车应用软件在提供相关汽车智能网联服务的同时，能够保障网联服务的安全可靠性，吉林省汽车电子协会联合各相关单位起草了系列标准。在本标准中，主要补充制定了移动终端控车应用软件信息安全相关的测试要求。

移动终端控车应用软件信息安全测试规范

1 范围

本文件规定了移动端控车应用软件信息安全测试要求，主要包括应用安全基本检测要求、敏感信息安全基本检测要求、账户安全基本检测要求、数据安全检测要求，通讯安全、WebView 客户端安全检测。

本文件适用于移动终端控车应用软件信息安全检测指导。

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 25056-2018 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 25069—2010 信息安全技术 术语

GB/T 30276—2020 信息安全技术 网络安全漏洞管理规范

GB/T 34975-2017 信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 35278-2017 信息安全技术 移动终端安全保护技术要求

GM/T 0014-2012 数字证书认证系统密码协议规范

3 术语和定义

GB/T 25069—2010、GB/T 35273界定的以及下列术语和定义适用于本文件。

3.1

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

[GB/T 35273—2020，术语和定义 3.1]

注：个人信息的范围和类型参见 GB/T 35273—2020 附录 A。

3.2

个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

[GB/T 35273—2020，术语和定义 3.2]

注：个人敏感信息的范围和类型参见 GB/T 35273—2020 附录 B

3.3

Android 移动端

指可以在安卓系统手机终端运行的应用软件。

3.4

iOS 移动端

指可以在苹果系统手机终端运行的应用软件。

3.5

Token 令牌

在计算机身份认证中是令牌（临时）的意思，一般作为邀请、登录系统使用。

3.6

SSL证书

SSL 证书是一种数字证书，主要是给予网站 HTTPS 安全协议加密传输与信任的功能。

3.7

Web Storage 浏览器存储

浏览器本地数据存储的一种方式。

3.8

Cookie小型文本文件

浏览器保存在客户机中的简单的文本文件。

3.9

Root 根用户

安卓系统用户可以获取操作系统的根用户权限。

3.10

file域 文件域

在单一安全策略下运行的一组文件实体。

3.11

Web SQL 浏览器数据库

客户浏览器端的结构化的关系数据库。

3.12

WebView 网页视图

用来显示 Web 网页的控件。

4 缩略语

下列缩略语适用于本文件：

API：应用程序编程接口（Application Programming Interface）；

App：移动互联网应用程序（Mobile Internet Application）；

HTML5：超文本标记语言（ HyperText Markup Language 5 ）；

IP：网络之间互联的协议（Internet Protocol）；

SDK：软件开发工具包（Software Development Kit）；

SMS：短信息服务（Short Message Service）；

URL：统一资源定位符（uniform resource locator）。

5 移动端应用程序安全检测

5.1 移动端安全包签名校验检测

检测方法：利用反编译工具、漏洞扫描工具等。

扫描检测移动端应具备真实性和完整性校验，并在运行时进行签名检验，校验后应不可重新打包签名。

5.2 移动端代码安全检测

检测方法：利用反编译工具、漏洞扫描工具等。

扫描检测移动端源代码的安全性，应不可被反编译，且进行混淆。移动端代码中不可存在以下安全问题，包括但不限于：

a) 口令或密钥等关键信息硬编码在代码或资源文件中检测；
b) 存在未知权限和冗余权限，包括但不限于 file 域访问权限等检测；
c) 代码或配置文件中应清除的测试信息，如口令、内部 IP、账号地址等检测。

5.3 应用程序加固安全检测

检测方法：利用反编译工具、抓包工具检测、漏洞扫描工具等。

检测移动端应具有抗逆向分析等安全性防护措施，应用不可被反编译，且能够防范攻击者对移动端程序的调试、分析和篡改。

5.4 调试安全检测

检测方法：利用反编译工具、抓包工具检测、漏洞扫描工具等。

移动端程序不可被调试，能够检测运行时设置调试检测及已防范注入措施。检测移动端应包含如下检测点：

a) 防止动态调试攻击。Android 移动端关闭危险权限检测，如日志开关；iOS 移动端加入反调试检测；
b) 关闭应用程序的备份恢复功能检测。Android 移动端关闭危险权限，如准许备份开关；
c) 关闭安卓各组件的权限检测。如需必要开启的，应对组件调用进行验证；
d) 关闭调试日志函数调用检测。如需必要开启的，应确保日志的输出使用了正确的级别。在发布版本中关闭涉及敏感数据的日志信息。iOS 移动端移除通过 NSLog 输出程序日志的代码信息。

5.5 检测 App 程序不可被 Root 的手机设备中运行

检测方法：利用反编译工具、抓包工具检测等。

检测手机在获取 Root 权限后，应不可以获取读取到其他应用的文件或者进程中的敏感信息， 如个人隐私信息等。

6 敏感信息安全基本技术要求检测

6.1 密钥与证书安全检测

检测方法：利用反编译工具、抓包检测工具等。

移动端应不可存在明文的证书和密钥。

6.2 日志安全检测

检测方法：人工检测、反编译工具检测、抓包工具检测、漏洞扫描工具检测等。
移动端运行时日志输出检测，客户端日志输出标志及函数检测。
移动端是否覆盖到每个用户的日志记录功能检测。

a) 检测包含但不限于记录用户的以下信息：
   1) 成功和失败登录、退出事件；
   2) 更改重要应用系统级参数或业务参数事件；
   3) 用户管理相关事件，比如用户的增删，权限的变更操作；
   4) 重要业务操作的执行；
   5) 重要数据的下载等。
b) 检测日志是否满足以下格式：
   1) 对于每一个事件，其审计记录应包括事件的日期和时间、IP 地址、访问者标识、事件类型、事件结果、变更事项等内容；
   2) 日志不应记录口令或密钥、客户支付敏感信息等重要数据。

6.3 隐私、敏感信息安全检测

检测方法：利用反编译工具、抓包工具检测等。

检测移动端应不存在明文的车辆控制伪指令、移动端通信 API 示例、服务系统 URL、用户敏感信息。敏感数据在显示时，应进行脱敏处理，如身份证号、手机号、住址等信息。且符合《移动互联网应用程序个人信息保护管理暂行规定》。且根据不同类型的 APP 隐私数据收集，明确数据收集边界应符合《常见类型移动互联网应用程序必要个人信息范围规定》中相关规定。

6.4 敏感个人信息安全检测

检测方法：人工检测等。

检测相关应用中，应包含隐私协议，且隐私政策中应包含保护个人信息的相关说明，APP 应具备保护个人信息的相关能力，对于个人信息的使用和收集，应在开始的页面予以说明。

7 账户安全基本技术要求检测

7.1 检测移动端应用登入业务逻辑-多点登录

检测方法：人工检测、抓包工具检测等。
应用不应支持同时多点登录。

7.2 检测移动端登入业务逻辑-防非法手机登入

检测方法：人工检测、抓包工具检测等。
应用不应支持利用非法手机号登录。

7.3 检测移动端登入业务逻辑-登入时防被窃取

检测方法：人工检测等。
应用应为自定义安全键盘，而非使用系统自带键盘。

7.4 检测移动端登入业务逻辑-账户窃取登入防护

检测方法：人工检测等。
应用应存在动态验证码。

7.5 检测移动端登入业务逻辑-短信验证

检测方法：人工检测、利用反编译工具、抓包工具检测、漏洞扫描工具检测等。

a) 验证码应存在发送时间限制，且不可为无限制快速发送；
b) 应用不可用任意验证码继续登录/其他业务逻辑；
c) 应用可防止篡改短信内容；
d) 验证码应有设置相应的失效机制；
e) 应用应能防止短信验证码绕过；
f) 服务端在验证短信验证码时，应能够防止越权校验。

7.6 检测移动端登入业务逻辑-调试接口关闭

检测方法：利用反编译工具、抓包工具检测、漏洞扫描工具等。
API 接口日志展示的功能应为关闭状态。

7.7 检测移动端登入业务逻辑-凭证暴力破解

检测方法：人工检测、反编译工具等。
检测应含有设定账户锁定策略，限制错误登录次数，且能够避免被暴力破解。

7.8 检测移动端登入业务逻辑-弱 token

检测方法：利用反编译工具、抓包工具检测、漏洞扫描工具等。
检测口令或密钥明文不应存放在配置和日志文件中。

7.9 检测移动端登入业务逻辑-凭证有效性

检测方法：人工检测、抓包工具检测等。
检测服务端应含有校验 Token 有效性，对于无效 Token 应禁用。

7.10 检测移动端注册安全

检测方法：人工检测、抓包工具检测等。
检测用户可重新注册(直接登录)，亦或列举已经注册用户。

7.11 检测汽车控制指令重放攻击

检测方法：利用反编译工具、抓包工具检测、漏洞扫描工具等。
检测截获/复制的控车指令重放后车端不应成功执行。

7.12 检测软键盘劫持

检测方法：利用反编译工具检测，人工检测、漏洞扫描工具等。

检测在应用内设置软件盘，应能防止用户在操作手机客户端等输入用户账户、登录口令或密钥、支付密码、资金操作等关键敏感信息时，被木马或黑客监听，导致用户输入的关键信息泄露。

8 检测数据通信安全基本技术要求

8.1 检测通信保密-安全协议

检测方法：抓包工具检测等。
检测关键连接应用应使用安全传输协议进行通信，如 TLS2.0 及以上版本。

8.2 检测通信保密-证书有效性

检测方法：利用反编译工具、抓包工具检测等。
检测客户端应能够对服务端 SSL 数字证书的合法性进行校验，校验失败采取退出客户端、注销会话等措施。

8.3 检测通信保密-关键数据加密

检测方法：利用抓包工具检测等。
关键数据在传输中应加密。

8.4 检测通信保密-数据合法性

检测方法：利用反编译工具、抓包工具检测、漏洞扫描工具等。
检测校验数据合法性，对数据进行数字签名等，应确保服务端下发的明文数据不被篡改。

9 通讯安全基本技术要求检测

9.1 检测程序中断-通讯

检测方法：人工检测等。
应用运行过程中，如有来电、SMS、蓝牙等通讯或充电情况，应能够可以暂停，优先处理通讯，并在处理完毕后正常恢复应用，继续原有功能。

9.2 程序中断-网络中断或异常检测

检测方法：人工检测等
创建网络连接或网络异常时，应用应能处理网络连接中断情况并告知用户网络已中断。

10 WebView 客户端、小程序、公众号、等技术要求检测

10.1 WebView 客户端安全

检测方法：利用反编译工具、抓包工具检测、漏洞扫描工具等。
检测应能够保证使用 WebView 方式开发的 APP 客户端软件的安全性。对于使用 WebView 方式开发的 APP 客户端，是否同时满足以下两点：

a) 不应明文保存用户名及口令或密钥。Android APP 设置 Web 是否关闭 WebView 组件的保存口令

或密钥功能；

b) 检测应能够防止 WebView File 同源策略绕过漏洞。

1) 检测应将不必要导出的组件设置为不导出，并先设置所注册组件的相关属性为 false；

2) 检测如果需要导出组件，应禁止使用 File 域；

3) 检测如果需要使用 File 协议，应禁止 File 协议调用。

10.2 Web Storage 数据泄露检测

检测方法：抓包工具检测、漏洞扫描工具等。

检测 Web Storage 中的多种存储方式下，本地存储信息中不应包含敏感信息，并且可被获取。

10.3 Cookie 信息泄露检测

检测方法：抓包工具检测、漏洞扫描工具等。

检测 Cookie 信息不应存储敏感信息，并且可被攻击获取，冒充管理者登录后台进行数据篡改等恶意操作。

10.4 WebSQL 注入漏洞检测

检测方法：抓包工具检测、漏洞扫描工具等。

检测应用中 HTML5 如在浏览器里面存数据库，应对用户输入的字符串进行过滤，转义，限制等处理，且不可通过输入构造的字符串去非法获取到数据库中的数据，并通过 SQL 注入点进行 WebSQL 攻击，从而导致存储的敏感数据信息被查询泄露。

10.5 集成 SDK 检测

检测方法：抓包工具检测、漏洞扫描工具等。

通过静态扫描等方式，检测出静态代码与 SDK 库特征代码进行比对，分析该代码是否属于某第三方 SDK，该 SDK 访问地址不应为三方服务器地址等。