

车机助手

第 1 期 MRD

审核人	
重要性	高
紧迫性	高
拟制人	牛兵帅
提交日期	2019/01/28
需求变更控制时间点	

修改记录

更新时间	变更内容	变更撰写	变更理由
2019.1.28	新建需求 v1.0	牛兵帅	
2019.3.15	新增隐私跳转入口	薛森	车控需求
2019.3.22	细化防火墙流量统计排序功能	薛森	功能描述细化
2019.05.14	隐私权限默认开启	薛森	客户需求
2019.07.02	流量统计长按 3S 功能	薛森	客户需求

注：提交评审之前的修改也可以记录下来

目录

目录

目录	3
一、 产品背景	4
1. 需求概述	4
2. 项目目标	4
二、 需求概览	5
1. Feature List	5
2. 页面描述	6
3. 威胁分类	7
三、 Story 详述	7
1. Story: 车机助手-S1 主页	7
2. Story: 车机助手-S2 防火墙	9
3. Story: 车机助手-S3 隐私	11
4. Story: 车机助手-S4 安全功能模块/服务说明	15

一、 产品背景

1. 需求概述

1) 背景介绍：

随着汽车智能化、网联化和电动化程度的不断提高，智能网联汽车信息安全问题日益严峻，信息篡改、病毒入侵等手段已成功被黑客应用于汽车攻击中，特别是近年来不断频发的汽车信息安全召回事件更是引发行业的高度关注。智能网联汽车的信息安全危机不仅能够造成个人隐私、企业经济损失，还能造成车毁人亡的严重后果，甚至上升成为国家公共安全问题。2017 年 6 月 1 日正式实行的《中华人民共和国网络安全法》要求智能网联汽车制造厂商、车联网运营商“采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。”为有效保障车机系统的网络安全，百度研发了车机系统的安全应用——车机助手。

2) 产品功能介绍：

本产品定位为车机 IVI 安全产品，可以兼容多款硬件平台及不同的安卓操作系统。通过监控及周期性检测系统应用的合法性，阻止恶意或未经授权的软件安装，检测并阻止可疑的网络连接及端口访问，保障车机系统和汽车联网的安全性；同时为方便用户对车内隐私的保护，支持用户关闭应用对定位服务及麦克风的访问权限。

3) 本文档的涵盖范围：

本文档覆盖福特项目相关的安全需求。

2. 项目目标

1) 作为安全模块，整体融合到小度车载 OS 里，搭载到福特项目中。交付内容包括 APK，sdk，bin 文件等，并提供友好的用户交互界面。

2) 软硬件环境：

- a) 硬件平台：i.mx8 Quad Max
- b) U-boot 版本：2017.03
- c) Linux Kernel 版本：4.9.69
- d) 安卓操作系统版本：8.1
- e) 车型及车机屏幕：

车型代号	车型名称	横屏竖屏	屏幕尺寸	分辨率	竖：横
CD391	福特蒙迪欧	竖屏	12.8	1920*1080	16:9
CX482	福特翼虎	横屏	12.3	720*1920	3:8
CX483	林肯 MKC	横屏	12.8	1080*1920	9:16
U611	林肯飞行家	横屏	12.8	1080*1920	9:16
U625	探险者	竖屏	12.8	1920*1080	16:9

- 3) 记录车机助手模块内各页面跳入跳出路径、时间数据，用于分析、改进产品。
- 4) 各类安全日志采集并上传到百度的服务器，用于分析、改进产品。

二、需求概览

1. Feature List

C 端用户可见部分

功能划分	功能描述	备注
车机监控防护显示 (launcher 卡片页)	纯色的防护图标，文案：“已安全守护 X 天”以及“>”可点击引导箭头。点击图标或文案区域，跳转到车机助手主页	更多规则请参考 launcher 页 MRD
车机防护 (车机助手主页)	车机防护动图	防护动效
	车机防护项	显示各防护项，包括：

		防火墙 APP 对外通信加密及双认证 数据防护
防火墙	流量统计	统计各应用的数据流量，WLAN 流量使用情况。维度：本月，上月，按照使用量排序
	联网防护记录	逐条显示联网防护的内容及处理结果 将防护记录加入白名单功能
隐私	隐私内容列表	包括定位服务、麦克风
	隐身模式	一键关闭所有应用对上述隐私内容的访问权限
	逐项隐私权限设置	逐个管理每个应用对上述隐私内容的访问权限

C 端用户不可见部分

功能/服务模块	描述
系统补丁	采用百度业界首创的热修复方案
操作系统配置安全	当前系统是否为 release 版 ADB 是否具有 Root 权限 系统是否可以被调试 符合福特提供的安全标准，具体实现方案参考相关设计文档。
非 root 操作	防止应用程序拥有 root 权限 检测系统是否有 root 工具
内存保护	开启内存保护机制
修复 CVE	根据确认的邮件分工，对百度用到的 open source software 中的已知 CVE 进行修复
代码混淆	采用百度加固方案
非授权应用安全	防止安装、运行非授权、被篡改的应用软件 保护授权应用不被非法卸载，篡改
应用沙盒	开启应用沙盒
SELinux	开启 SELinux
隐私	对麦克风、GPS 数据的非法访问进行监控
PKI	百度提供 PKI
TEE 数据安全	数据安全防护 SDK 密钥、证书安全存储 SDK
安全 OTA	云端安全包制作及车端安全包校验
通信安全	关键业务实现通信双向认证，并使用 TLS1.2 通信协议
车端安全日志	包括异常网络链接、非授权 App 事件、隐私数据非法访问及 OTA 升级异常
云端安全日志	车端安全日志上传到云端，并进行安全存储 云端安全日志传输到车厂

2. 页面描述

页面编号	页面划分	说明	备注
------	------	----	----

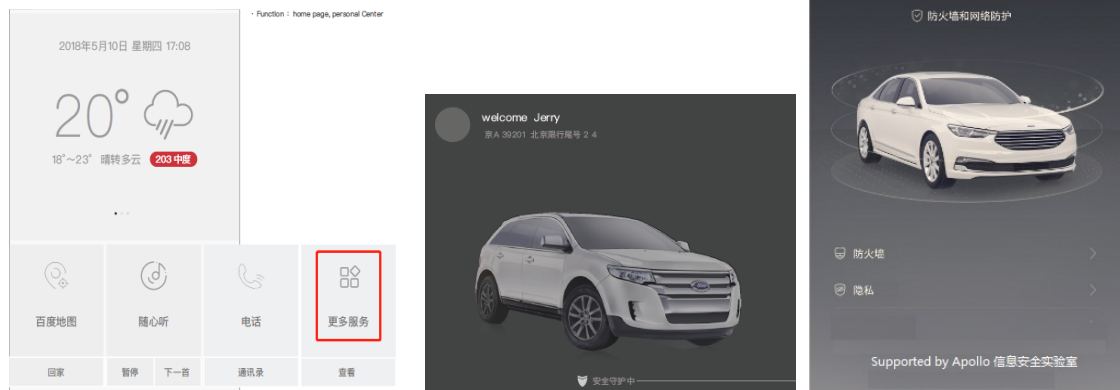
0	Launcher 车辆状态 卡片页	车机监控防护显示	
1	主页	车机助手 APP 主页，上下滚动显示监控防护信息；子模块功能入口	
2	防火墙	包括流量统计及联网防护记录	
3	隐私	隐身模式 各应用对定位服务、麦克风的访问控制	

3. 威胁分类

SN	威胁类型	描述	威胁等级	处理结果
1	APP 应用安全	非授权应用安装、执行 授权 APP 的卸载	中	需要记录相关日志。
2	OTA 升级安全	车机端篡改包的安装	中	阻止篡改包的安装，并记录相关日志
3	异常网络访问	不在 IP,APP 网络访问策略规则里的网络连接	中	阻止、断开连接，并记录相关日志
4	隐私访问	对用户 GPS 及麦克风的访问记录	低	记录相关的异常访问日志

三、Story 详述

1. Story: 车机助手-S1 主页



通过点击车机首页的更多服务，或 launcher 车辆状态卡片页中防护图标或文案，或通过“系统设置”中“隐私设置”进入隐私主页，或通过语音的交互“查看/打开/进入车机助手页面”或“查看/了解车机助手”，进入车机助手主页面；通过语音“查看/进行隐私设置”进入隐私主页；“查看流量情况”进入防火墙主页；车机助手主页分为以下三部分：

1.1 车机防护信息显示

需要显示的信息如下：

SN	显示内容	信息类型	规则描述	后台实现的内容
1	√ 防火墙和网络保护	防护信息	固定文案	IP 规则策略管理 APP 规则策略管理 异常网络访问连接检测及阻断
2	√ 车机对外通信安全防护	防护信息	固定文案	应用程序与服务器之间的交互使用安全通信协议（如 TLS1.2）以及双向认证机制
3	√ 数据安全防护	防护信息	固定文案	数据防篡改，数据防伪造，数据加解密 SDK

1.2 功能模块入口

主要包括防火墙以及隐私。

1.3 文字信息展示“Supported by Apollo 汽车信息安全实验室”

2. Story: 车机助手-S2 防火墙

防火墙主要通过进行策略的配置管理，实现了内核层及应用层的网络防护。同时对车机端应用的流量进行统计并记录日志，并对用户付费流量的应用进行显示。防火墙主页默认显示流量统计的内容。可在车机首页或车机助手首页，通过语音进入流量统计页面。语音内容：“查看流量使用情况”。C 端可见部分主要有下功能：

2.1 流量统计

统计用户付费的各应用的流量使用情况，包括 WLAN 以及蜂窝移动数据。统计周期为当月及上月的使用情况，并按照使用量，由大到小排序。默认按照蜂窝数据排序，当用户点击 wlan，按照 wlan 排序，当用户点击蜂窝数据，按照蜂窝数据排序。页面如下：

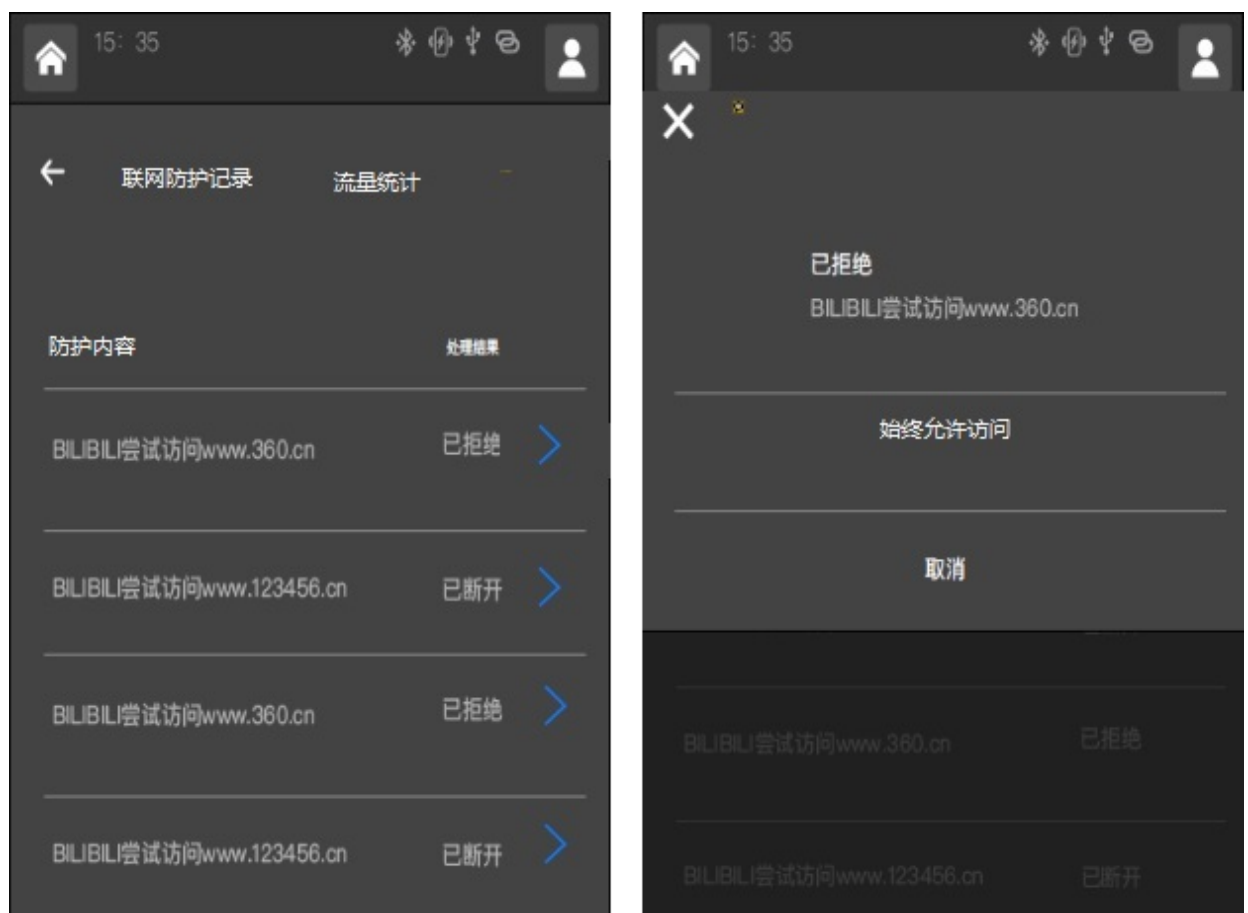


为便于用户理解，在该页顶部增加常驻文案“您的运营商对流量的计算方式可能与本设备的计算方式不同。”当无流量消耗时，页面显示文案为“无流量使用记录”。如果本月和上月均无流量消耗，页面中【本月】【上月】【WLAN】【蜂窝移动数据】标签不进行显示。

应用图标和应用名称应该与车机 OS 中的图标和名称一致，比如：“随心看”。如果和用户交互的部分没有这个应用，不在流量统计中显示；用户长按 3S【流量统计】显示所有进程流量使用情况；如果该应用包含在其它 APP 中，显示整体，而不是其中的部分。

2.2 联网防护记录

联网防护记录列出了不在网络配置规则内的网络连接及处理情况。合法的网络连接基于车机端规划的业务，在 SOP 前完成全部策略配置。用户可以将其中的某些网络连接设置为允许访问网络，设置过程需要进行弹窗确认。设置完成后，后台更新对应配置规则，并立即生效。可在车机首页或车机助手首页，通过语音交互进入联网防护记录页面。语音内容：“查看联网防护记录”。联网防护记录的页面如下：



联网防护记录为空时的文案为：防护记录为空，未发现可疑的联网行为。

页面元素说明

元素	说明	备注
返回	点击跳转到车机助手模块主页	
联网防护记录	当前页面名称	
防护内容	显示连接访问的对应域名	
处理结果	显示对联网防护记录的处理结果	已拒绝；已断开
防护信息列表	显示全部的防护信息	
始终允许访问	可以对任一防护记录设置始终允许访问网络	

联网防护记录需要记录日志并上报到百度自己的云端服务器。具体日志要求及上报策略在日志管理系统设计文档中描述。日志上报成功后对本地日志进行删除。

3. Story: 车机助手-S3 隐私

隐私模块是查看和管理各应用对用户车内隐私的使用权限的统一入口。主要包括定位服务以及车内麦克风。第一次使用车机，隐身模式默认关闭，定位和麦克风隐私防护列表中的权限默认开启。所有隐私项，在 launcher 页或车机助手主页均可通过语音进行开关控制，如“开启/关闭 GPS（定位服务）”，“开启/关闭麦克风”；完成相关控制后，进行对应的语音播报，如“已开启/关闭 GPS 访问权限”，“已开启/关闭麦克风访问权限”。隐私页面如下

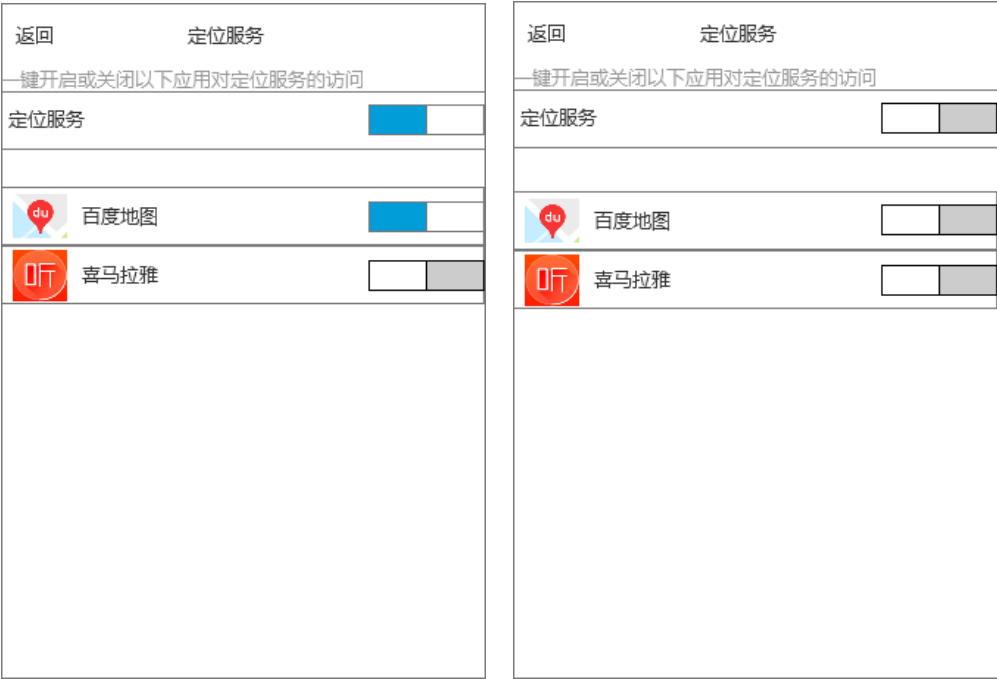


页面元素说明

元素	说明	备注
返回	点击跳转到车机助手模块主页	
隐私	当前页面名称	
隐身模式	默认关闭。用户一键开启后，则关闭所有隐私设备和信息的应用访问权限；用户一键关闭，则恢复原来的权限访问设置。	
文案描述	开启后，相关应用将不能访问您的以下隐私数据	
隐私列表	隐私内容名称，开关状态，可点击引导图标 “>”	点击后进入各隐私项的单独设置页面。见 3.1，3.2


3.1 定位服务

查看和管理各应用对定位服务的访问权限。可以对每个应用单独进行设置，也支持一键关闭所有应用对定位服务的访问。一键打开时，恢复原来的权限访问设置。页面如下



页面元素说明

元素	说明	备注
返回	点击跳转到隐私主页	
定位服务	当前页面名称	
文案描述	开关开启的时候，文案：已开启以下应用对定位服务的访问权限 开关关闭的时候，文案：已关闭以下应用对定位服务的访问权限	
“定位服务”， “  ”图标	定位服务一键开关。状态为“关闭”时，列表内所有应用无法使用定位服务。	当有至少一个应用的开关为“打开”状态时，一键开关为“打开”状态；当所有应用的开关为“关闭”状态时，一键开关为“关闭”状态

应用列表	应用图标，应用名称，“  ”图标， 所有申请了“定位服务”访问权限的应用	
------	--	--



3.2 麦克风

查看和管理各应用对麦克风设备的访问权限。可以对每个应用单独进行设置，也支持一键关闭所有应用对麦克风设备的访问。页面如下



页面元素说明

元素	说明	备注
返回	点击跳转到隐私主页	
麦克风	当前页面名称	
文案描述	开关开启的时候，文案：已开启以下应用对 麦克风的访问权限 开关关闭的时候，文案：已关闭以下应用对	

	麦克风的访问权限	
“ 麦 克 风 ” ，  图标	麦克风一键开关。状态为“关闭”时，列表内所有应用无法使用麦克风。	当有至少一个应用的开关为“打开”状态时，一键开关为“打开”状态；当所有应用的开关为“关闭”状态时，一键开关为“关闭”状态
应用列表	应用图标，应用名称，“  ”图标， 所有申请了“麦克风”访问权限的应用	

4. Story: 车机助手-S4 安全功能模块/服务说明

4.1 密钥及证书

支持 ford 密钥标准和密钥注入交换流程，支持 ford 证书。

4.2 安全 OTA

云端安全包制作及车端安全包校验，主要包括如下内容。具体实现方案参考相关设计文档。

云端安全包制作	升级包加密
	升级包签名（支持福特签名）
	身份认证
	升级包防拷贝签名
	身份 Token 生成
	安全升级包制作
车端安全包验证	升级包防重放
	升级包解密
	升级包验证签名

	升级包鉴定来源可信
	升级包防拷贝验签
	升级包双向身份认证（在线升级）
通讯通道	支持 HTTPS/TLS 协议