



2023 年 车企 App 安全研究白皮书

北京顶象技术有限公司

2023 年 6 月

目录

一 车企 App 面临双重风险	4
1.1 车企 App 的技术威胁	5
1.1.1 ROOT 风险	5
1.1.2 模拟器攻击风险	6
1.1.3 验证码爆破风险	6
1.1.4 系统 API Hook 风险	6
1.1.5 代理环境风险	6
1.1.6 反编译风险	6
1.1.7 二次打包风险	6
1.1.8 通信风险	7
1.1.9 密码爆破风险	7
1.1.10 so 文件风险	7
1.1.11 签名校验风险	7
1.1.12 动态调试风险	7
1.1.13 进程注入风险	7
1.1.14 数据明文储存风险	7
1.1.15 Logcat 日志风险	8
1.1.16 任意文件上传风险	8
1.1.17 SQL 注入风险	8
1.1.18 XSS 漏洞风险	8
1.2 车企 App 合规风险	8
二 车企 App 遭遇威胁攻击的原因	9
2.1 从封闭到联网的变化	9
2.2 软件与通信的漏洞	10
2.3 攻击者愈加专业	10
三 车企 App 安全解决思路	11
3.1 监管指导建议	11
3.2 技术解决思路	12
3.2.1 安全加固	12
3.2.2 安全检测	12
四 车企 App 安全方案	12
4.1 App 加固	12
4.2 App 隐私合规检测	13
五 基于虚机源码保护的顶象 App 加固	13
5.1 顶象 App 加固介绍	13
5.2 虚机源码保护技术	14
5.2.1 运作流程	14
5.2.2 技术特点	15
5.3 顶象 App 加固后的安全性能	15
六 汽车行业案例	16
助东风雪铁龙防范黄牛党	16
保障飞凡汽车 App 安全	17



保障神州优车 App 账户安全 17

保障理想汽车用户账户安全 17

增强如期出行营销服务品质 17

保障比亚迪售后服务系统安全 17

助力 T3 出行防范营销欺诈 17

七 附录 18

 关于顶象 18

 联系我们 19



一 车企 App 面临双重风险

自有 App 成为各品牌汽车的标配，也成为车企必争的新战场。车企 App 不仅能够实现远程开启空调、门锁、启动车辆等功能，还提供购车、购买配件、维修、保养等基础服务，更承载着优化车主用车体验、构建品牌私域流量池的新任务，成为车企与用户关系运营的重要渠道。

车企 App 最核心的功能可以概括为三个部分：服务、社区、商城。服务是用户使用 App 的基础需求；商城通过积分兑换提升用户粘性，通过商品售卖进行获利；社区则承担了增强用户粘性，提高用户活跃的重要功能。随着“以用户为中心”的市场战略和运营策略也在加快落地，车机互联、车友社区、购物娱乐等功能不断完善，车企 App 用户规模实现快速增长。

品牌	APP	品牌	APP	品牌	APP
特斯拉	特斯拉	小鹏	小鹏	斯柯达	大众斯柯达
保时捷	保时捷	蔚来	蔚来	雪佛兰	My chevy
奔驰	Mercedesme	理想	理想	宝骏	宝骏车联
路虎	路虎	长安	长安	海马	海马
林肯	林肯之道	现代	现代	奔腾	yomi
凯迪拉克	My cadillac	领克	Lynkco	威马	威马智行
红旗	红旗智联	哈弗	哈弗智家	别克汽车	别克汽车ibuy
吉利	吉利汽车	极氪	极氪	名爵	mglive
比亚迪	比亚迪汽车	WEY	Wey道	江淮	江淮汽车
马自达	My mazda	上汽奥迪	上汽奥迪	宝沃	宝沃
一汽大众	一汽大众	上汽大众	上汽大众	长城欧拉	欧拉ora
一汽丰田	一汽丰田	上汽荣威	上汽荣威	捷途	捷途
一汽奥迪	一汽奥迪	广汽本田	Wowstation	标志	东风标致智行
雷克萨斯	Elexusclub	广汽传祺	传祺	雪铁龙	东风雪铁龙智行
东风本田	东风本田	广汽埃安	埃安	飞凡	r汽车
东风风神	风神	广汽三菱	广汽三菱	捷豹	捷豹车主专享
零跑	零跑	日产智联	日产智联		

除了以上服务，对车辆软硬件的操控，如解锁车门、升降车窗、远程启动、查看车辆行驶轨迹或当前位置等最“原始”的功能。

随着车企 App 成为汽车交互的主要入口之一，隐私、安全问题频频爆出。随着智能网联技术逐步完善，汽车网络安全的各种隐患也逐步浮现出水面，车企 App 需要应对各种威胁。

2022 年 4 月，通用汽车通报检测到了恶意登录活动，黑客在某些情况下将客户奖励积分兑换为礼品卡，针对此次事件，通用汽车也及时给受影响的客服发邮件并告知客户。当年 12 月，蔚来汽车就用户数据遭窃取发表致歉声明，证实了此前其用户数据被泄露的传闻，并表示公司承诺对因数据泄露给用户造成的损失承担责任。





此外，监管部门对保障 App 用户合法权益非常重视，自 2019 年来，联合开展 App 专项整治工作，与 App 治理相关的法律文件也相继出台。违法违规的 App 不仅收到监管机构的通报批评，还面临被下架等监管处罚。

总体来说，汽车 App 面临两重风险：技术威胁、合规风险。

1.1 车企 App 的技术威胁

一辆智能网联汽车每天会产生大约 10TB 的数据，驾乘人员的出行轨迹、驾乘习惯、车内语音图像等个人信息都面临着被泄露的风险。攻击者可以通过网络漏洞攻击劫持或控制车辆行驶，实施关闭引擎、突然制动、开关车门等操控。数据显示，2020 年全球针对智能网联汽车的攻击达到 280 余万次。

综合来看，车企 App 主要以下安全威胁。

1.1.1 ROOT 风险

Root 代表绝大部分移动设备的使用者能够掌握到的最高权限，使用户拥有了修改系统文件的权限，甚至可以控制账户、增加或删除硬件等。在 ROOT 环境下，App 可以随意访问任意



应用储存的任何数据，造成数据泄露、数据非法篡改等风险。

1.1.2 模拟器攻击风险

模拟器是一种“仿真”程序，可以在电脑模拟出一个独立的手机环境，最初是用于开发过程中调试、测试、模拟运行等。模拟器可以让攻击者监控应用关键函数、获取应用敏感数据、破解应用的目的，也可以采用多开方式手动操作或是结合模拟点击，成为黑灰产牟利的工具。

1.1.3 验证码爆破风险

用户使用手机号+验证码的方式进行登录时，短信验证码大部分情况下是由 4~6 位数字组成，如果没有对验证码的失效时间和尝试失败的次数做限制，攻击者就可以通过尝试这个区间内的所有数字来进行暴力破解攻击。同时，如果没有对验证码的发送次数进行限制，可以对同一手机号或者不同手机号无限次发送，存在恶意调用接口发送短信的风险，造成短信发送平台花费大量的短信费用，且易造成骚扰短信，影响用户的正常使用。

1.1.4 系统 API Hook 风险

Hook 技术是一门广泛用于计算机攻防对抗的技术。可以监视系统或者进程中的各种事件消息，截获发往目标窗口的消息进行处理。攻击者利用 hook 手段对 App 进行脱壳、内存截取/修改等操作。

1.1.5 代理环境风险

App 应用运行在代理环境下，通信过程能被中间人截获，造成用户请求伪造、重放攻击、敏感信息泄露等威胁。

1.1.6 反编译风险

反编译就是逆过程，高级语言源程序经过编译变成可执行文件，反编译出的 App 代码未做任何保护，信息数据、功能流程等都被暴露，攻击者能够完整地分析 App 的运行逻辑，尤其是相关业务接口协议、和通信加密的实现，给业务带来极大的风险。

1.1.7 二次打包风险

使用 apktool 对 App 进行解包，添加自定义的代码，回编译后，将 App 重新安装到手机中可以正常运行。App 被轻易的二次打包，很容易被攻击者添加恶意的代码或者添加广告，从而窃取登录账号密码、支付密码等，严重威胁用户隐私安全，也给公司的形象带来不利的影响。



1.1.8 通信风险

App 与服务器进行交互时，使用不安全的 HTTP 协议，或关键数据明文传输，或互相不验证证书，攻击能够窃听、篡改、统信数据甚至篡改，进而影响数据的安全性，或者发动中间人攻击。

1.1.9 密码爆破风险

App 上的用户账号，如果密码简单存在被暴力破解风险；如果如果没有对登录错误次数、请求时间进行校验，同时密码等敏感数据未进行加密处理，则可遭遇暴力破解的风险。

1.1.10 so 文件风险

so 文件是 Linux 下的程序函数库,即编译好的可供其他程序使用的代码和数据。攻击者可以通过工具进行破解，使用调试工具对其动态调试，分析代码中的业务逻辑以及加密算法。

1.1.11 签名校验风险

App 签名机制是对 APK 包完整性和发布机构唯一性的一种校验机制，需要对 APK 进行签名后才能后进行安装。大部分的安卓 App 没有对正盗版进行校验，重新签名后的 App 在手机中安装后可以正常运行，车企 App 面临被攻击者二次打包、恶意篡改、山寨的风险。

1.1.12 动态调试风险

App 在运行的过程中，攻击者通常会使用调试器对程序进行动态调试，如果 App 未做防动态调试保护，则程序运行过程中，攻击者可以通过动态调试技术，利用 gdb/ida 等调试工具对程序进行内存调试跟踪，可以窃取目标进程的数据信息，从而获取用户的隐私数据信息。

1.1.13 进程注入风险

如果程序本身对运行时的内存没有做任何的保护措施，攻击者通过反编译对源代码进行分析，定位到可以程序外 Hook 类似操作的关键位置，完全不需要修改程序本身，当程序运行到敏感的界面 Activity 时，从程序外获取用户输入的证件号、姓名、手机号和密码等敏感的信息，并从内存中进行修改，尤其是对于涉及到支付等操作时，将严重威胁用户的财产安全。

1.1.14 数据明文储存风险

车辆 VIN、安全码、车辆所有者等敏感信息如果直接明文存储在数据库或其他存储介质中，而不加任何加密或哈希处理。攻击者可以使用这些 token 来获取授权或模拟用户身份进行恶



意操作。

1.1.15 Logcat 日志风险

App 在运行的过程中，如果日志的输出没有做好等级控制，查看日志时，用户名、密码等敏感信息可能被泄露。

1.1.16 任意文件上传风险

很多 App 具有文件上传功能，如果服务器对用户文件上传部分的控制不足或者处理缺陷，导致用户可以越过其本身权限向服务器上传可执行的恶意脚本文件，从而控制服务器，造成重要数据的丢失。

1.1.17 SQL 注入风险

如果 App 在编写时没有对用户提交至服务器的数据的合法性进行校验，可以将 SQL 命令插入到 Web 表单进行提交，从而达到欺骗服务器执行恶意 SQL 命令的目的，实现对数据的任意读写，造成核心机密数据被窃取和篡改的安全风险。

1.1.18 XSS 漏洞风险

在使用投诉、建议等功能时，如果在 App 编写时没有对用户输入数据的合法性以及在将数据输出到网页时数据的合法性进行校验，攻击者可以向 Web 页面里面插入恶意 JavaScript、HTML 代码，并且将构造的恶意数据显示在页面，从而泄露客户端的 cookie 或者其他敏感信息。

车企 App 一旦出现安全风险，将会给汽车造成难以估量的安全威胁，严重危及财产安全乃至生命安全。未知攻焉知防，只有先了解有哪些风险才能够有效防范。

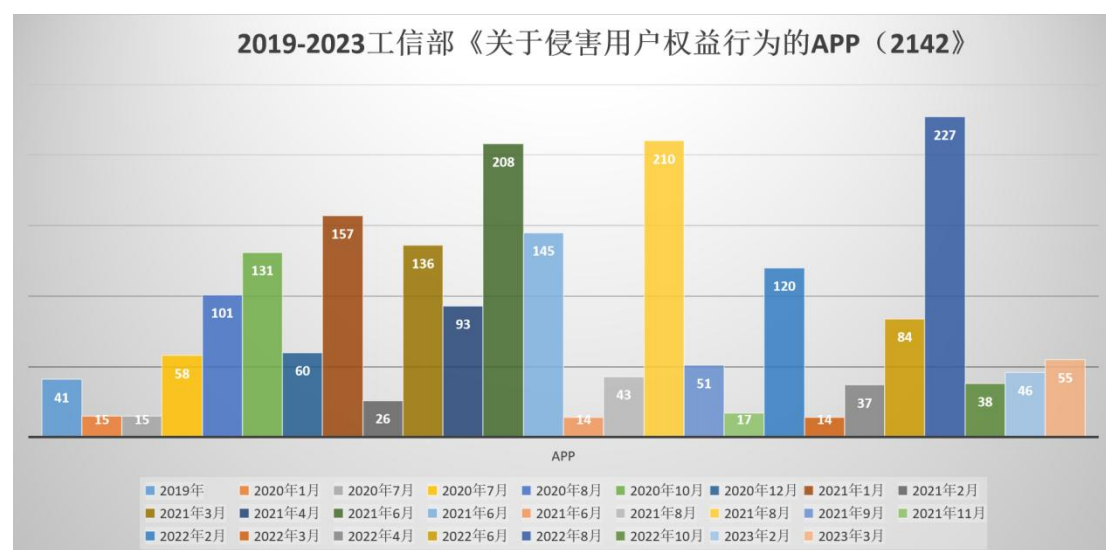
1.2 车企 App 合规风险

2023 年，工业和信息化部通报了 2023 年第 2 批侵害用户权益行为的 App（SDK）名单，共有 55 款 App 被通报，涉及强制、频繁、过度索取权限等问题。这些 App 存在着一些消费者难以察觉的问题，如频繁自启动和关联启动、超范围索权、应用分发平台信息不到位等，给用户的安全和隐私带来了风险。

根据 2019 年到 2023 年《关于侵害用户权益行为的 App》通报显示，共有 2142 款 App/SDK 遭到处罚。这些 App 主要存在违规收集、使用用户个人信息、不合理索取用户权限、为用户账号注销设置障碍等问题，严重侵犯了用户的隐私和合法权益，给用户的生活和工作带来了不小的影响。



为了解决以上问题，工业和信息化部正在加强监管力度，多次发布关于侵害用户权益的通知和指导意见，并按照《网络安全法》、《个人信息保护法》等法律法规，对违规行为进行打击和处罚。



二 车企 App 遭遇威胁攻击的原因

媒体不完全统计，2019 年，攻击者通过入侵汽车 App、改写程序和数据的方式，盗走包含奔驰 CLA、GLA 小型 SUV、Smartfortwo 微型车在内的 100 多辆汽车。相比于以盗窃汽车为目的的黑客攻击，智能汽车在网络安全和行驶过程中遭到黑客攻击带来的危险性显然更为严重。

知名汽车网络安全公司 UpstreamSecurity 发布的 2020 年《汽车网络安全报告》显示，自 2016 年至 2020 年 1 月份，汽车网络安全事件增长了 605%，仅 2019 年一年就增长 1 倍以上。按照目前的发展趋势，随着汽车联网率的不断提升，预计未来此类安全问题将更加突出。

2.1 从封闭到联网的变化

车联网的概念源于物联网，即车辆物联网，是以行驶中的车辆为信息感知对象，借助新一代信息通信技术，实现车与 x（即车与车、人、路、服务平台）之间的网络连接。车联网能够提升车辆整体的智能驾驶水平，为用户提供安全、舒适、智能、高效的驾驶感受与交通服务，同时提高交通运行效率，提升社会交通服务的智能化水平。

汽车原本没有考虑联网需求，随着汽车产业向智能化、网联化、共享化、电动化为特征的“新四化”方向狂飙迈进，汽车不再只是孤立的交通工具，而是成为融入互联互通体系的信息终端，车与车、终端应用、路边基础设施以及云端之间的联通也随之大大增强，由此导致更多的信息安全接入点和风险点被暴露出来。业务、数据、用户信息、运营过程等均处于边界模



糊且日益开放的环境中，存在各类风险。

伴随着新能源汽车的蓬勃发展和互联网+空间的延伸，以及新一代信息通信技术的发展，车联网从简单的车机系统逐步成长为汽车和外界之间的网络连接平台和大脑。数字化、网联化、智能化的发展趋势已经成为未来汽车业转型升级的方向，也让智能化车辆驾驶和决策成为可能。

车联网采用了传感器、处理器等大量的设备，但是其硬件安全远没有我们想象的那么安全。从汽车钥匙、车载娱乐系统到远程信息处理器，可逆向的点多如牛毛，通过硬件逆向而入侵系统的事件比比皆是。车联网设备种类繁多，厂商的安全意识薄弱，大多关注功能叠加，较少有安全防护措施。同时，设备上使用的操作系统，大多基于开源的操作系统改编过来，厂商依赖于这些操作系统本身的进步来增强安全性，通常不会积极主动提供升级的能力。

2.2 软件与通信的漏洞

资料显示，一辆智能汽车的车载智能设备数量不小于 100 台，所有程序代码不小于 5000 万行，因此整个智能驾驶代码将达 2 亿多行。Karamba Security 公司首席执行官阿米·多坦曾表示：“每 1800 行代码就存在一些错误，其中 80%是安全漏洞。一辆联网汽车和一辆自动驾驶汽车的潜在安全漏洞数目分别为 5000 和 15000。其中，自动驾驶汽车的代码可能超过 3 亿行，这大约是拥有 1500 万行代码的波音 787 梦幻客机的 20 倍。可以说，自动驾驶汽车是目前最复杂的运输平台。”

众所周知，代码数量越是庞大，软件越是复杂，那么其中包含的漏洞就越多，由此被攻击的概率也就越高。按照目前汽车平均拥有一亿行代码来计算，每辆智能汽车就可能存在 10 万个缺陷或漏洞。而这些缺陷以及漏洞会造成什么样的风险，没有人可以预测。漏洞是威胁的爆发源头，无论是病毒攻击还是黑客入侵大多是基于漏洞，业务、软件、系统、设备都要漏洞，只是有的被发现的没被发现。软件漏洞、接口漏洞、管理漏洞等等。

2.3 攻击者愈加专业

网络攻击者呈现专业化、产业化、组织化的形态，他们熟悉业务流程以及防护逻辑，能够熟练运用自动化、智能化的新兴技术，不断开发和优化各类攻击工具，不断发起各类攻击。

2021 年机械工业出版社出版的《攻守道-企业数字业务安全风险与防范》一书和中国信通院 2022 年发布的《业务安全白皮书》中有详细地分析：网络黑灰产彼此分工明确、合作紧密、协同作案，每一环节都有不同的牟利和运作方式，形成一条完整的产业链。以大规模牟利为目的网络黑灰产，熟悉业务流程以及防护逻辑，能够熟练运用自动化、智能化的新兴技术，不断开发和优化各类攻击工具，不断发起各类欺诈攻击。

相关数据显示，目前网络黑灰产从业人员近 200 万之众，每年造成的损失达数千亿元。



三 车企 App 安全解决思路

汽车企业应该加强自身 App 的安全保障措施，确保用户数据的安全和隐私不受侵犯。企业应该制定完善的信息安全管理制度和流程，对员工进行安全教育和培训，采用安全的技术手段和方法，有效防范和打击恶意攻击、恶意软件等安全威胁。

3.1 监管指导建议

《网络安全等级保护 2.0》

“应采用密码技术保证通信过程中数据的完整性”；“应对移动终端应用软件恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等”

《移动金融客户端应用软件安全管理规范》

客户端应用软件应具备基本的抗攻击能力，能抵御静态分析、动态调试等操作。客户端代码应使用代码加壳、代码混淆、检测调试器等手段对客户端应用软件进行安全保护。客户端应用软件安装、启动、更新时应应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。

《移动金融客户端应用软件安全检测规范》

“检查客户端软件是否可以抵御静态分析、动态调试；是否使用技术手段对客户端软件进行安全保护；是否具有保持自身完整性、真实性，防止篡改及注入的功能；输入控件是否具有抵御一定程度攻击的能力；是否具有已知漏洞的防范能力等”。

“检查客户端应用软件是否具有检测运行环境的能力，是否在检测到运行环境处于 ROOT 或者已越狱、非可信环境（如模拟器或虚拟机）等异常环境时向后台系统反馈设备环境信息等”。

《网上银行系统信息安全通用规范》

客户端程序在启动和更新时应进行真实性、完整性校验（例如，联机动态校验等），防范客户端程序被篡改或替换。客户端程序应采取代码混淆、加壳等安全机制，防止客户端程序被逆向分析，确保客户端的敏感逻辑及数据的机密性、完整性。客户端程序应保证自身的安全性，避免代码注入、缓冲区溢出、非法提权等漏洞。



3.2 技术解决思路

3.2.1 安全加固

针对 App 普遍存在的破解、篡改、盗版、调试、数据窃取等各类安全风险提供的有效的安全防护手段，其核心加固技术主要包含防逆向、防篡改、防调试及防窃取这四大方面，不仅保护了 App 自身安全，同时对 App 的运行环境及业务场景提供了保护。

3.2.2 安全检测

通过自动化检测和人工渗透测试法对 App 进行全面检测，并挖掘出系统源码中可能存在的安全风险、漏洞等问题，帮助开发者了解并提高其应用开发程序的安全性，有效预防可能存在的安全风险。

四 车企 App 安全方案

4.1 App 加固

App 加固能够为 App 提供移动应用运行进行安全监测，对移动应用运行时终端设备、运行环境、操作行为进行实时监测，帮助 App 建立运行时风险的监测、预警、阻断和溯源安全体系。

全方位保障 App 安全。能够针对已有应用进行安全性检测，发现应用存在的风险漏洞并针对性进行修复整改，对敏感数据、代码混淆、代码完整性、内存数据等进行保护，从源头上避免系统漏洞对于应用本身造成的安全影响，保障 App 信息安全。

为 App 提供实时风险预警。能够为 App 提供移动应用运行进行安全监测，对移动应用运行时终端设备、运行环境、操作行为进行实时监测，帮助 App 建立运行时风险的监测、预警、阻断和溯源安全体系。

为 App 建立全生命周期防控体系。App 应用安全加固呈现常态化、泛边界化和专业化的趋势，这意味着企业自身简单的防护已经无法满足当前网络安全防护的新趋势，亟待建立更为全面的安全防御体系。顶象端加固从 App 的设计、开发、发布、维护等全生命周期环节解决移动应用在核心代码安全、逻辑安全、安全功能设计、数据传输链路安全等多个维度的问题，助力筑牢安全防线。



4.2 App 隐私合规检测

App 隐私合规检测服务帮助开发者发现 App 可能存在的各类隐私安全漏洞，提供详细的检测报告，并给出专业的合规整改建议。同时，顶象专业的隐私安全专家团队，还为开发者提供一对一专家咨询服务，帮助开发者高效检测，快速识别 App 潜在的隐私风险，构建安全可信的高质量 App。

App 隐私合规检测服务可以应用于上架前和合规检测。

App 上架前隐私检测。在各个移动应用市场在应用上架前，对 App 进行隐私检测，确保安全合规、发现存在的风险。

App 合规检测。基于多个监管文件，进行 App 日常合规检测、整改、二次检测和抽检等，防止对客户信息过度收集。

应用隐私合规检测服务提供个人信息保护现状，威胁定位分析和可视化结果报告。

五 基于虚拟机源码保护的顶象 App 加固

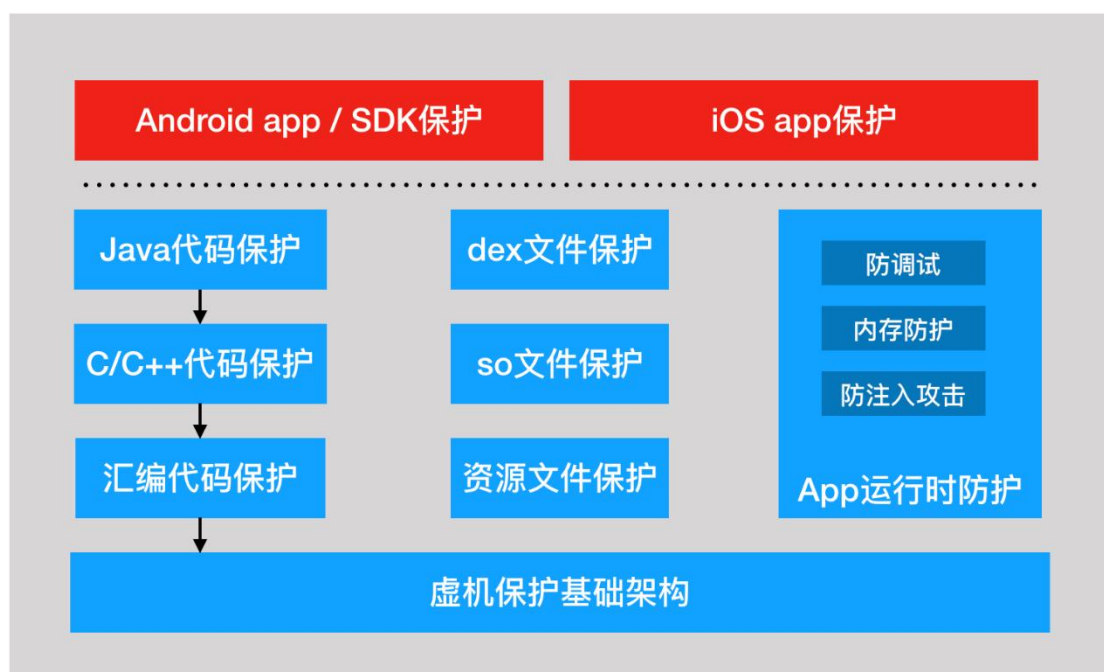
5.1 顶象 App 加固介绍

顶象 App 加固基于虚拟机源码保护技术，良好兼容 Java、Kotlin、C/C++ 等多种语言。可以保护 Android 的 DEX、配置、SO 等 16 种数据和文件安全，可有效侦测对抗动态调试、代码注入、内存 dump、root 环境、多开环境、模拟器、重打包等风险。

顶象 App 加固提供了一套完整的工具链，首先把 App 代码编译成中间的二进制文件，随后生成独特的虚拟机源码保护执行环境以及只能在该环境下执行的运行程序。也就是虚拟机源码保护会在 App 内部隔离出独立的执行环境，该核心代码的运行程序在此独立的执行环境里运行。即便 App 本身被破解，这部分代码仍然不可见。

顶象 App 加固通过技术和管理手段来增强实际系统的安全防护能力，可以通过自身的探针感知到环境的变化，实时探测到外界对本环境的调试、注入等非正常执行流程变化，将调试动作引入程序陷阱，并发出警报，进而进行实时更新，进一步提高安全强度。此外，顶象 App 加固率先支持对 iOS 免源码加固，提供代码混淆、字符串混淆、符号混淆、指令虚化、防调试、反编译、防 Class dump 的保护，并支持 Bitcode 输出。





产品架构

5.2 虚拟机源码保护技术

机源码保护是顶象完全自主知识产权的技术，对 App、IoT 等进行安全加固。虚拟机源码保护将核心代码编译成中间的二进制文件，随后生成独特的虚拟机源码保护执行环境，将所有高风险操作在该环境内执行，操作完成环境立即释放，不给攻击者可乘之机。

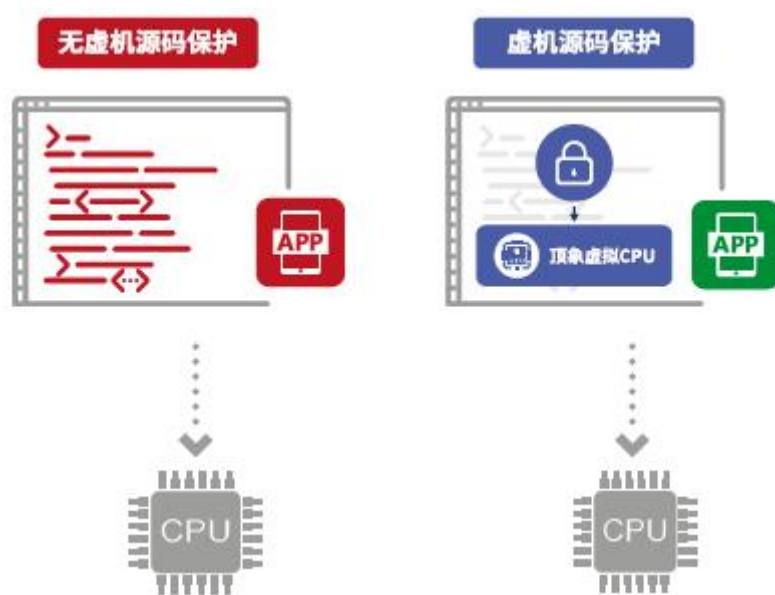
5.2.1 运作流程

在准备阶段，虚拟机源码保护为用户提供一套完整的工具链，首先把用户待保护的核心代码编译成中间的二进制文件，随后生成独特的虚拟机源码保护执行环境和只能在该环境下执行的运行程序。

在 App 运行阶段，虚拟机源码保护会在 App 内部隔离出独立的执行环境，该核心代码的运行程序在此独立的执行环境里运行。

生成的虚拟机源码保护拥有独特的可变指令集，极大的提高了指令跟踪、逆向分析的难度。同时，虚拟机源码保护还提供了反调试能力和监控能力。虚拟机源码保护可以通过自身的探针感知到环境的变化，实时探测到外界对本环境的调试、注入等非正常执行流程变化，将调试动作引入程序陷阱，并发出警报，进而进行实时更新，提高安全强度。





5.2.2 技术特点

代码虚拟化：在运行时使用顶象独创的虚拟 CPU 直接运行加密的代码。这些加密的代码完全不同于常见的 x86 或 ARM 指令，从而任何逆向工具均无法直接逆向破解。

一机一密的安全性：为每位用户动态生成不同的加密指令，大大增加逆向破解的难度。

保护强度更高：源码保护提供比传统加固更健壮的保护强度，从编译过程开始保护代码中的核心逻辑、关键算法、重要数据结构。

良好的兼容：源码级别保护不使用任何操作系统未公开的 API，不使用任何系统版本升级可能引起的不稳定机制，受保护的代码仍经正常编译打包流程生成 App，避免兼容性问题。

全平台支持：不仅 Android、iOS 双平台支持，还支持各种定制化操作系统甚至无操作系统的 IoT 设备。支持包括 Java，Kotlin，C/C++，Objective-C，Swift 等在内的多种语言。

5.3 顶象 App 加固后的安全性能

字符串加密：将 App 的源代码中敏感字符串做随机加密处理。在运行时进行对字符串动态解密，这样就可以避免攻击者，通过利用工具进行静态逆向分析发现关键字串信息，从而快速定位到应用中的业务代码。

控制流平坦化：将 so 文件中 C/C++ 代码中的执行控制逻辑变换为平坦的控制逻辑，从抽象语法树层面进行深度混淆，使得其在常用反编译工具中，极大的降低反编译逆向代码的可读性，增加逆向代码的分析难度。



指令替换：对代码中的运算表达式进行等效转换，使其在常用反编译工具中，提高破解者逆向分析门槛，有效的保护核心算法的原始逻辑。

局部变量名称混淆：对源代码中的变量名称进行做混淆操作，混淆后变量名称变成无任何意义的名称。这给分析者加大了分析强度。

符号混淆：对 App 应用中的类名称、函数名称进行混淆操作，增大直接用工具分析难度，让反编译逆向工具，无法直接通过类名称、函数名称进行快速定位 App 的核心代码。

混淆多样化：采用在混淆过程中引入随机性技术，在相同的混淆策略下，每次混淆后的代码均不一致，进一步提升攻击者通过利用工具进行静态分析的难度。

不透明谓词：将代码中分支跳转判断条件，由原来的确定值变为表达式，增加程序逻辑的复杂性、降低代码的可读性。

防动态调试：对 App 应用进行防调试保护、检测到配置防动态调试功能的类、方法、函数被 IDA 逆向工具进行动态调试时候，App 应用进行自动退出运行操作，有利于保护 App 应用直接被动态调试，从而提高攻防对抗的门槛。

防动态注入：对 App 应用进行防动态注入保护，当利用 `zygote` 或 `ptrace` 技术进行 App 应用的注入操作时，App 应用进行自动退出运行操作，以此进行防御攻击方对 App 应用的非法操作，避免动态分析执行代码，从而达到动态保护 App 应用安全。

HOOK 检测：对 App 进行防 HOOK 保护，检测到配置防 hook 保护功能的类名、方法名、函数名在被 `frida`、`xposed` 等工具动态 hook 时候，App 进行自动退出操作，以此进行提高防御 App 安全性，保护 App 不被注入攻击，抵御恶意侵入。

代码段检验：对 App 应用中的代码段进行完整性校验，发现代码段被篡改，App 应用进行自动退出运行，防止 App 应用中的代码逻辑被篡改，以此进行动态保护 App 的源代码安全性。

完整性校验：对 App 中指定的函数级进行完整性校验，当应用被重新签名和代码的完整性遭到破坏时候，检测点进行触发 App 程序闪退，以此抵御主流的调试器调试分析，从而达到动态保护程序安全。

六 汽车行业案例

助东风雪铁龙防范黄牛党

东风雪铁龙大降价，官方小程序吸引了大批黄牛党。配置了拥有风控能力的顶象无感验证验证码，拦截大批欺诈异常账号，让黄牛不能成功抢购，保障了消费者合法权益。



保障飞凡汽车 App 安全

为了进一步保障 App 安全，飞凡汽车部署顶象 App 加固。能够有效防御内存注入、Hook、调试、注入、多开、内存 Dump、模拟器、二次打包和日志泄露等攻击威胁，防止 App 遭受入侵、篡改、破解、二次打包等恶意侵害，并能够对密钥存储文件、配置类文件的进行加密，保障隐私数据安全。

保障神州优车 App 账户安全

针对神州优车的恶意抢单行为，顶象智能无感验证有效识别各类机器行为，实时拦截垃圾注册、批量登录等风险操作，防范恶意抢单、薅羊毛等欺诈手段。基于顶象无感验证，平台可以进一步对恶意用户进行账号冻结、账号注销等方式进行处置，从而进一步保障了平台业务健康有序。

保障理想汽车用户账户安全

为了防范各类账户风险的发生，理想汽车引入了顶象智能无感验证，有效防范垃圾注册、撞库攻击、暴力破解等风险，保障用户账户安全，实现了用户体验与业务安全的良好平衡。

增强如期出行营销服务品质

如祺出行部署顶象无感验证，用于新人券、周末打折券等各类促销活动中。无感验证能够根据用户的行为和设备信息，快速准确地区分操作者是人还是机器，及时甄别出羊毛党的机器账号，实时监控并拦截恶意行为，能够有效防止羊毛党刷单、哄抢等行为，避免大量机器账号的恶意攻击，保障真正消费者的权益。

保障比亚迪售后服务系统安全

为了加强售后服务平台的安全性和防范欺诈行为，比亚迪售后服务平台选用顶象无感验证。顶象无感验证技术可以快速准确地区分操作者是人还是机器，精准识别欺诈行为，及时甄别出恶意账号，避免大量机器账号的恶意攻击，实时监控并拦截异常行为，保障登录过程的安全性。

助力 T3 出行防范营销欺诈

T3 出行为司乘准备的优惠福利，让大批“羊毛党”闻风而动。在顶象的助力下，T3 出行及时发现并拦截一大批哄抢优惠券、打折卡、限时免费、新手大礼包的“薅羊毛”欺诈团伙，保障用户、司机的合法权益，提升平台的推广精准度，为业务健康发展提供有利保障。



七 附录

关于顶象

顶象是国内领先的业务安全公司，旨在帮助企业构建自主可控的业务安全体系，解决伪造、篡改、劫持、冒用、虚假制作等业务欺诈威胁，防范化解各类网络黑灰产风险，让业务更加健康稳定，助力企业创新与增长。

顶象自主研发了一站式业务安全感知防御云，包括设备指纹、智能无感验证、实时决策、端加固、安全感知防御平台等产品，通过在银行、电商、航空、出行、游戏、教育、旅游、媒体、政务、智能制造等行业积累了丰富的实战经验，沉淀了数万条业务策略和数百个场景化应用方案，能够为企业构建覆盖事前、事中、事后全生命周期的安全体系，提供情报、感知、分析、策略、防护、处置等服务。

顶象总部位于中国北京，在杭州、南京、广州、深圳、上海、成都、西安、济南设有分部，是 CNNVD（国家信息安全漏洞库）、CICSVD（国家工业信息安全漏洞库）、CNCERT（国家互联网应急中心）技术支撑单位和信创工委会会员单位，先后获得红杉资本、嘉实投资、晨兴资本、东方弘泰资本的数亿元投资。

截止 2022 年，顶象已为 24 个行业、3000 多家企业提供专业服务。





联系我们

邮件: marketing@dingxiang-inc.com

电话: 400-8786123

网址: www.dingxiang-inc.com

