ColorOS 11 安全技术白皮书

2020年 8 月

目录

1 总述

随着移动互联网飞速发展，智能移动终端逐渐普及、渗透和融入人们的工作和生活。现代的智能移动终端是由多种软硬件组成的复杂系统，在提供给用户社交、购物、支付、出行、娱乐等丰富体验地同时，来自硬件、系统、应用、网络等多层面多维度的安全威胁随之产生，终端用户对于数据安全、隐私保护的诉求越来越凸显。

OPPO 以用户数据安全和隐私保护为核心，建立了完善的内控体系和权限管理流程，实现用户数据存储加密，传输加密，敏感数据去标识化，全方位保护用户的数据与隐私。ColorOS 作为 OPPO 手机操作系统，在设计时即考虑构筑全面的终端安全架构，进行了大量安全和体验性的功能创新，为用户提供端到端的安全保护,旨在为用户提供最高的安全和透明体验。同时 OPPO 获得业界第一个工信部泰尔实验室信息安全新五级认证，该认证证明 OPPO 终端从硬件安全、系统安全、外围接口安全、应用软件安全、用户数据安全等层面，提供了全面的安全防护。

图 1-1　ColorOS 安全架构

ColorOS 以硬件信任根为起点，利用安全启动（Secure Boot）和 Android 启动验证（Verified Boot）机制在"信任根-引导加载程序-系统启动分区"等组件之间建立起完整信任链传递关系。在设备启动过程中，无论哪个阶段，在进入下一个阶段之前先验证下一个阶段的完整性和真实性，确保系统从硬件芯片到系统启动的安全。在系统安全方面，ColorOS 基于 Verified Boot，结合 SELinux、内核防 Root、系统软件更新等机制防止恶意篡改和非法访问，保障系统安全；在应用安全方面，通过应用安全检测、应用签名校验、安全沙箱、运行时保护等安全机制保障应用从上架、安装、运行整个阶段的安全性。

在硬件、系统、应用安全的基础上，ColorOS 开发了一系列安全特性提供拦截检测、支付保障、数据保护、隐私控制等业务安全能力，从而进一步保护用户业务及数据的安全。

本文详细介绍了 ColorOS 安全性技术和功能，希望可以帮助用户和安全从业人员清晰地理解 ColorOS 安全架构与安全解决方案。本文主要分为以下几个章节：

- 硬件安全：包括可信执行环境、安全启动，防回滚等；
- 系统安全：包括可信启动、SElinux、内核防 root、漏洞缓解、系统软件更新等 ；
- 通信与网络安全：包括 TLS、VPN、WLAN、WIFI 安全检测、防伪基站等；
- 应用安全：包括应用威胁检测、应用签名、应用沙箱及运行时保护机制等；
- 拦截检测：包括骚扰拦截、恶意网址检测；
- 支付保障：包括 OPPO Pay、支付保护中心、短信验证保护等；
- 设备管理：包括查找手机、远程守护、儿童空间等；
- 数据安全：包括安全存储、可信 UI、密钥管理、文件系统加密（FBE）、数据擦除、锁屏密码保护、指纹保护、安全键盘、密码本等；

- 隐私控制：包括系统分身、权限管理、保护个人信息、隐私行为提醒、位置服务、应用锁&应用隐藏、私密保险箱等。

2 硬件安全

硬件安全是整个终端安全的基础，为 ColorOS 提供底层的硬件安全支撑。ColorOS 通过可信执行环境 TEE、安全启动，防回滚机制（Anti-rollback）等特性和服务来保障上层的系统、应用、数据及业务安全。

2.1 可信执行环境

可信执行环境（TEE, Trusted Execution Environment）是基于芯片级隔离技术，用于保证程序执行安全与数据存储完整性、机密性和真实性为目标构建的一种可信赖的软件运行环境。TEE 为 ColorOS 提供安全服务，使用户的关键数据在这个相对可信赖的环境中使用和运行。

图 2-1　可信执行环境

搭载 ColorOS 的终端设备基于芯片级隔离技术建立两个执行环境。其中，一个环境负

责处理对功能性、开放性等要求较高的业务，即富执行环境（REE, Rich Execution Environment），如上图的 ColorOS 执行环境。另一个负责处理对安全性、私密性要求比较高的业务，即可信执行环境。ColorOS 执行环境中的客户端应用可以与可信执行环境中的可信应用相互交互和协作完成对用户敏感数据的保护。

构建可信执行环境主要涉及硬件和可信软件两方面：

（1）硬件资源隔离

硬件资源隔离是构建可信执行环境的基础。用户的敏感信息可能存储在设备中的 CPU、内存、外设等硬件资源中，这些硬件资源在芯片级安全隔离机制基础上严格隔离。

（2）构建可信软件架构

在硬件安全扩展的基础上，构建可信软件架构，软硬件相结合提供一个安全的软件执行环境。

1）系统软件层：

提供了可信操作系统基本核心功能，包括进程调度管理、时间管理、中断管理、进程间通信管理和外设驱动管理；

提供了可信操作系统的系统级功能，包括用户态和内核态的定义，系统调用访问控制和权限管理；

充分利用安全硬件（如一次性可编程存储（OTP）、重放保护内存块（RPMB）、安全元件、硬件加密引擎等）的可信性，完成安全存储、安全加解密等各种系统服务；

可信操作系统与 ColorOS 之间的通信采用共享内存或消息方式；

2）应用软件层：

各种安全相关的可信应用，如指纹、支付、身份认证等，一般与对应的 ColorOS 应用交互，为用户提供既便捷又安全的用户体验。

2.2 安全启动

硬件的安全启动是系统利用签名公钥确保文件或程序完整性安全机制。在启动过程的任何阶段，所有启动程序（包括启动引导程序、内核镜像、基带固件等）必须通过签名公钥校验才可以加载运行，否则启动过程会被终止，以防止加载并运行未经授权的程序。

设备开机后，最先执行一段在芯片制造时被写入芯片内部只读 ROM 中的引导程序，称为片内引导程序（ROM SoC Bootloader），该程序在芯片出厂后无法修改，为硬件信任根。片内引导程序执行基本的系统初始化，从 Flash 存储芯片中加载一级引导程序，并使用保存在主芯片内部 Fuse（用户空间文件系统）空间的公钥进行一级引导程序镜像的数字签名校验，校验成功后运行一级引导程序。一级引导程序加载、校验和执行 TEE OS 及二级引导程序镜像，然二级引导程序加载、验证和执行下一个镜像文件。以此类推，直到整个系统启动完成，保证启动过程的信任链传递，防止未授权程序被恶意加载运行。

ColorOS 基于平台的 Secure Boot 架构，优化了其中的密钥管理策略、签名验证策略和下载认证策略，使得安全启动在 ColorOS 上更加的安全和稳定。通过 ColorOS 安全启动功能，提升了的安全性，包括但不限于：

- 禁止烧写未经授权的官方固件；

- 禁止运行非经授权的官方固件；
- 禁止非法追踪和调试代码，例如 JTAG（Joint Test Action Group）接口和故障转储；
- 对单个芯片设定 IMEI；
- 禁止不同设备（芯片、型号、版本等）固件的交叉写入；
- 对内部而言：密钥管理策略更加安全和保密，以最小权限为原则。普通工程师无法接触和获取到密钥。

2.3 防回滚

ColorOS 支持防回滚（Anti-rollback）功能，在每台设备的主芯片内部 Fuse 空间中烧写 Anti-Rollback 值，同时在镜像签名中新增 Anti-rollback 值。在 Secure Boot 鉴权签名的阶段，对 Anti-Rollback 进行检测，防止固件或者镜像降级烧入设备，避免引入低版本漏洞。

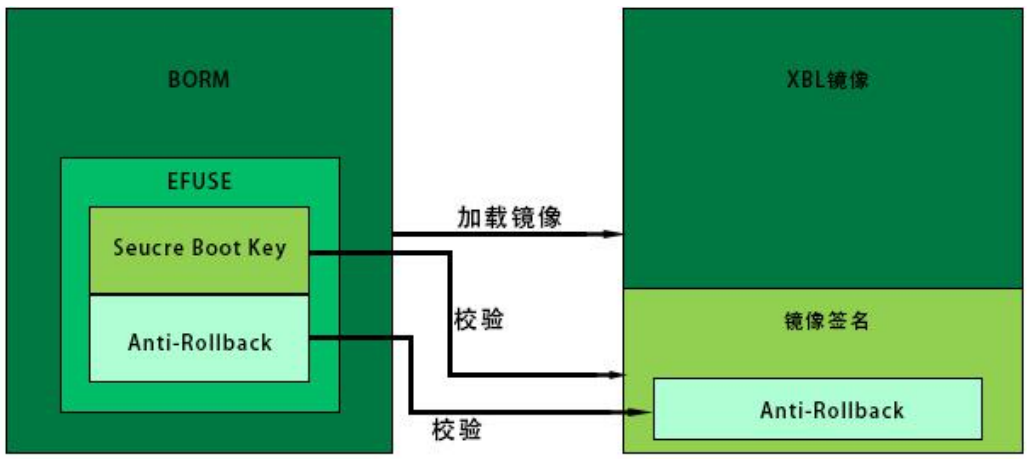

图 2-3　防回滚机制

3 系统安全

系统安全在硬件安全的基础上，结合 SELinux、内核防 Root、系统软件更新等机制防止系统被恶意篡改和非法访问，保障系统安全，主要从可信启动、SELinux、内核防 Root、漏洞缓解、内核热修复、系统软件更新等几个方面构筑 ColorOS 系统安全能力

3.1 可信启动

Android Verified Boot（AVB，安卓启动验证）是保证终端用户设备上运行的软件的完整性的安全机制。在 Secure Boot 的基础上，以通过已被鉴权的 LK（little kernel）镜像为起点，以信任链的方式确保镜像的合法性和完整性，防止篡改相关镜像入侵系统的行为，提高系统的抗攻击能力。

Secure Boot 和 Verified Boot 结合建立一条从信任根到引导加载程序，再到启动分区和其他已验证分区的完整信任链。在设备启动过程中，无论是在哪个阶段，都会在进入下一个阶段之前先验证下一个阶段的真实性和完整性。

ColorOS 支持 AVB 功能，增加了对 Boot、Recovery、System、Vendor 等镜像完整性和合法性的检测。同时，在 Android P 版本后，可信启动的校验增加了防回滚功能。

3.2 SELinux

SELinux（安全增强性 Linux）是 Android 安全模型的一部分，Android 使用 SELinux 对所有进程强制执行强制访问控制。ColorOS 支持 Android 原生的 SELinux 特性，通过预定义强制访问控制策略实现进程权限的控制，将进程对系统中的目录、文件、

进程等资源的操作权限最小化，防止绕过内核安全机制的攻击或未授权的数据读写，确保 Android 内核及上层应用的安全运行。

3.3 内核防 Root

ColorOS 致力于为用户提供安全可靠的操作系统，在内核层面上，ColorOS 根据内核非法 Root 后的特征行为设计了动态防御机制，以此来抵御恶意的 Root 手段。CorlorOS 将持续对此进行优化，为用户提供更加安全的操作系统。

3.4 漏洞缓解

在堆栈溢出攻击中，攻击者常常通过覆盖函数的返回地址来绕过数据执行保护（Data Execution Prevention，DEP）技术来达到攻击目的，这种攻击依赖显式跳转地址。而地址空间配置随机加载（Address space layout randomization，ASLR）技术通过随机放置一些关键数据的地址空间避免了这种攻击。

ColorOS 支持 KASLR 特性，该特性使内核在内存地址空间的位置不可预测，使得攻击代码无法找到内核位置，防止内核漏洞被利用，降低遭到复杂攻击的可能性，提升系统安全性。

ColorOS 支持 PAN/PXN 特性，其中 PAN（Privileged Access Never，特权模式访问禁止）实现内核态不允许访问用户态应用的数据的效果，防止高权限的内核窃取应用的数据；PXN（Privileged Execute Never，特权模式执行禁止）特权模式不可执行，防止在内核态模式下直接跳转到用户态的代码段进行提权攻击。

3.5 系统软件更新

ColorOS 定期发布系统安全补丁，并提供 Android 原生的 OTA（Over the Air，空中下载）机制，方便用户及时修复可能存在的漏洞。当用户通过 OTA 升级时，系统首先检验升级包的签名，只有校验通过的升级包才被允许安装。ColorOS 提供系统软件更新管控，防止系统软件更新到低版本存在的漏洞，给设备造成风险。

4 通信与网络安全

ColorOS 采用业内标准网络协议并提供数据加密传输。提供 Wi-Fi 安全检测功能保障用户网络接入安全。提供防伪基站安全功能，减少不良来电和诈骗短信。

4.1 TLS

TLS（Transport Layer Security，传输层安全协议）通过在传输层对网络连接进行加密，为网络通信提供安全及数据完整性的一种安全协议。

对于 TLS/SSL 协议，ColorOS 支持更安全的 TLSv1.2、TLSv1.3。

4.2 VPN

VPN（Virtual Private Network，虚拟专用网）是在公网上使用隧道协议构建的点对点安全连接。用户可以通过 VPN 在共享或公共网络上实现安全的数据传输。

ColorOS 支持 PPTP、L2TP/IPSec PSK、L2TP/IPSec RSA、IPSec Xauth PSK、IPSec Xauth RSA、IPSec Hybrid RSA 等协议类型。同时 ColorOS 支持 PPP 加密（MPPE）。

4.3 WLAN

ColorOS 提供 WEP、WPA/WPA2 PSK/WPA3 PSK、802.1x EAP、WAPI 等多种 WLAN 认证方式，满足用户不同安全级别的需求， 有效提高无线网络通信的安全。

为防止监听器根据设备真实 MAC 地址生成设备活动的历史记录，ColorOS 默认使用随机分配 MAC 地址扫描并连接 WLAN 网络，从而加强对用户隐私的保护。用户可因个人

需要手动设置选择使用真实设备 Mac 地址。

同时 ColorOS 设备的 WLAN 功能默认关闭，一旦被用户开启，默认使用 WPA2 PSK 认证方式，保证连接安全。

4.4 WiFi 安全检测

用户在公共场所连接的 WiFi 可能存在一定安全风险。ColorOS 设备在连接到 Wi-Fi 后，会结合 DNS（Domain Name System，域名系统）、IP 等风险库对该网络环境进行安全检测，能够检测包括虚假（钓鱼）Wi-Fi、DNS 劫持、ARP 欺骗攻击。若检测到风险，则向用户发出警告。

为了有效避免连接公共场所 WiFi 存在的安全风险，ColorOS 设备基于大数据的机器学习技术，在用户在连接到公共场所 WiFi 后，对连接的网络环境进行多维度安全检测及判断，一旦确认虚假（钓鱼）WiFi、DNS 劫持、ARP 欺骗等攻击风险，则立即向用户发出警告，提示用户当前 WiFi 不安全，建议用户断开连接。

4.5 防伪基站

近年通过伪基站进行诈骗手机用户钱财的案件呈增长势头，不法分子利用伪基站干扰屏蔽运营商信号，使用户手机连接上伪基站信号，继而冒充他人手机号码、特服号码等任意电信网码号向用户发起垃圾短信、钓鱼诈骗、中间人劫持等攻击。

为了避免用户接入伪基站遭受损失，OPPO 针对性的研发出一套独家的基于 modem 芯片级的伪基站防御方案，提供伪基站的拒绝服务攻击防御、降级攻击防御、超时攻击防御及 GSM 伪基站防御等能力，实时启动芯片级识别防御算法自动分析系统广播参数和伪

基站行为特征，对伪基站进行识别和防御。

*注：上述功能仅适用于在中国和印度销售的 OPPO 手机。

5 应用安全

ColorOS 通过应用威胁检测、应用签名校验机制、应用沙箱机制和运行内存保护机制，保证应用从安装到运行的全阶段安全。

5.1 应用威胁检测

OPPO 软件商店是官方的应用和游戏的下载及管理平台，提供安全的内容丰富的各类应用。OPPO 软件商店严格把控上线应用的安全，在应用上架前必须全部通过开发者资质审核、App 资质审核、自动化安全查杀、人工审核 4 个环节的检测程序，应用才会能上架。对于已上架的应用，实施 24 小时在线监控，并配合安全查杀工具自动回扫机制，定期人工复检，一旦检测到 App 存在病毒、木马等可能威胁用户安全地风险，则自动下架处理。OPPO 软件商店保证向用户提供安全可靠的应用，建议用户从 OPPO 软件商店下载应用。

第三方未知来源（非 OPPO 软件商店）的应用未经安全检测，默认情况下禁止安装，以避免病毒木马等不必要地风险。ColorOS 允许用户手动开放未知来源应用的安装权限，并在第三方来源的应用安装时，对其进行安全性检查。同时，通过 USB 或其他途径保存到手机的 APK 应用安装包，ColorOS 也会对其进行安全性检查，以降低用户安全风险。

ColorOS 系统集成了多个知名安全厂商的病毒查杀引擎，提供本地及云端查杀能力，确保设备在有无联网的情况下都能发现应用的安全风险。病毒查杀引擎支持应用安装时检测和闲时体检，用户可在手机管家中手动触发设备病毒扫描功能，对恶意应用和恶意文件进行扫描。系统也提供后台自动体检功能，根据用户选择的自动体检频率（默认 1 天）触发后台体检任务。

*注：中国区版本集成安全厂商病毒查杀引擎，不同机型配置不同的主引擎。

5.2 应用签名

应用签名是一种校验机制，用以保证应用合法性和完整性 ColorOS 要求所有应用的安装/升级必须具有完整、有效的签名。

在程序安装时，ColorOS 对应用签名进行验证，以检查应用程序是否被篡改，验证不通过则不允许安装。

为了防止已安装应用被恶意应用通过升级的方式替换，ColorOS 要求新旧版本应用程序必须使用同一个证书进行签名，否则 ColorOS 认为是不同的程序，阻止应用升级。

5.3 应用沙箱

ColorOS 支持应用沙箱机制，利用基于用户的 Linux 保护机制来识别和隔离应用资源，将应用程序置于"沙箱"之内，实现应用程序之间的隔离，并设定允许或拒绝 API 的调用权限，限制应用程序对资源的访问，保护应用和系统免受恶意应用的攻击。

应用程序运行在它们自己的 Linux 进程上，在安装时被分配一个唯一的用户 ID 并永久保持，默认情况下对其他应用程序完全隔离。特殊情况下进程间可通过 Android 提供的共享 UID 机制建立相互信任关系，具备信任关系的应用程序可以运行在同一进程空间。

5.4 运行时保护

ColorOS 继承了 Android 的地址空间布局随机化（ASLR）和数据执行保护特征（DEP）保护运行时内存。ASLR 通过对堆、栈、共享库映射等线性区布局的随机化，有效防止攻

击者定位攻击代码位置，提高攻击者在利用内存漏洞上的难度，达到阻止溢出攻击的目的。

DEP 能将内存中特定区域标记为非可执行区域，以有效防止内存漏洞攻击。

6 拦截检测

拦截检测是 ColorOS 针对电话骚扰、短信及浏览器中恶意网址威胁提供的安全功能，对用户电话、短信及浏览器使用场景进行安全及隐私保护。

6.1 骚扰拦截

ColorOS 支持通话和短信骚扰拦截功能，提供隐藏号码拦截、疑似诈骗电话拦截、骚扰电话拦截、广告推销电话拦截、房产中介拦截等多种拦截能力，并且可以针对诈骗短信、广告短信进行智能识别和拦截，能够有效拦截各种营销诈骗电话、垃圾短信和广告短信，减少骚扰电话、短信带给用户的困扰。

骚扰拦截功能提供自定义拦截规则和拦截强度设置，并支持黑名单、白名单拦截机制，最大限度满足用户的拦截需求。

6.2 恶意网址检测

ColorOS 提供 OPPO 浏览器和短信中的网址安全检测功能，可分辨潜在威胁，减少挂马网站、色情网站、暴力网站、诈骗网站等恶意网站给用户带来的影响。

使用 OPPO 浏览器浏览网页时，系统将网址与内置网址信息库进行比对，若网址比对结果存在风险，OPPO 浏览器会提醒用户该站点存在安全风险并建议停止访问。

ColorOS 的短信应用提供在线识别恶意网址的功能，能够及时反馈短信中网址链接的安全性，对垃圾短信、诈骗短信进行标注，使用户能够直观感知。

7 支付保障

ColorOS 致力于保障用户的支付安全。本章介绍了 ColorOS 在自有支付软件（OPPO Pay）中对于安全所做的努力、以及为第三方支付 App 的所做的安全性支持。OPPO Pay 在用户、商家和发卡机构之间搭建了安全且私密的支付桥梁，支付过程并不会收集用户的任何交易信息。

7.1 OPPO Pay

OPPO Pay 是钱包提供的手机支付服务。用户在受支持的 OPPO 终端设备通过 OPPO Pay 绑定银行卡即可享受安全、便捷的支付体验。使用 OPPO Pay，手机秒变银行卡，可用于线上支付、线下 POS 机支付及地铁公交出行等应用场景。为保证支付安全，在硬件层面，OPPO 手机提供支付指纹信息的硬件加密与银行卡信息的安全存储，实现支付信息的物理隔离；在系统软件层面，发起支付时会自动检测支付环境是否安全可靠。

OPPO Pay 组件

安全单元（ Secure Element，SE ）：是经过工业标准认证的、运行在 Java Card 平台（Java Card Platform，JCP）、符合金融行业电子交易要求的安全元件。安全元件在带有近距离无线通信 NFC（Near Field Communication）模块的手机 OPPO 手机中存在。

NFC 控制器：NFC 控制器负责处理 NFC 协议，支持应用程序处理器和 SE 之间以及 SE 和销售点终端之间传输信息。

OPPO Pay 应用：在支持 OPPO Pay 的设备上承载该服务的应用指“钱包”，用户可以在钱包中添加和管理银行卡，及查看添加的卡片和发卡机构提供的其他信息（如设备卡号、最近的交易明细等）。

OPPO Pay 服务器：OPPO Pay 服务器负责管理 OPPO Pay 中的银行卡的状态，以及储存在 SE 中的设备卡号，同时与设备以及支付网络中的服务器进行通信。

OPPO Pay 如何使用 SE

手机 SE 中有专门管理 OPPO pay 的应用，或通过与支付网络或发卡机构认证的小程序，来实现与支付网络或银行卡发卡机构之间数据安全传输。加密后的银行卡数据安全存储在储存在 SE 中。交易期间，销售点终端使用专门的硬件总线通过 NFC 控制器直接与 SE 进行通信。

OPPO Pay 如何使用 NFC 控制器

作为 SE 的入口，NFC 控制器确保所有非接触式支付交易都通过处于设备近距离范围内的销售点终端进行。NFC 控制器只会将来自射频场内终端的支付请求标记为非接触式交易。当用户使用指纹或密码授权支付，NFC 控制器会将安全元件 SE 准备的非接触式响应专门发送给 NFC 射频场。交易的支付授权详细信息通过 SE 加密后直接发送给支付网络，不会透露给应用程序处理器。

添加银行卡

用户在 OPPO Pay 中添加银行卡时，需要使用银行卡号、卡片有效期、CVV 码等信息来进行绑卡验证。用户可以在钱包中手动输入或使用摄像头来识别填充银行卡号信息。

银行卡号信息输入完成后，OPPO 钱包会将卡号发送到 OPPO Pay 服务器再透传到发卡机构进行验证。验证通过后，OPPO 钱包将向用户返回银行协议，仅当用户同意后才能继续添加流程。用户后续填写的银行卡其他信息，将通过"银联可信安全服务控件"加密后发送到 OPPO Pay 服务器，并再次由 OPPO Pay 服务器透传给发卡机构。同时，OPPO 还会与发卡机构共享设备型号、SE 号，以及添加银行卡时用户大致位置（如果用户当前启用了"定位服务"）。发卡机构将会依据这些信息来决定是否批准将银行卡添加到 OPPO Pay。

支付授权

SE 仅在接收到来自手机的授权，确认用户已使用指纹或支付密码认证后，才会允许进行支付。如果开启了指纹支付，指纹即为默认的支付方式，指纹验证有效性只限当次交易，若用户失败次数超过系统指纹连续识别上限，将暂停指纹验证对该卡的操作，提示用户使用支付密码进行支付。

暂停使用或移除银行卡

用户可以登录 OPPO 钱包，手动移除已添加的银行卡。也可退出 OPPO 账号从而锁定银行卡将其置为不可用状态。针对已添加的"OPPO Pay 银行卡"，即使设备未接入网络，发卡机构或支付网络也可停用其支付功能，用户可通过致电发卡机构来暂停使用或移除该银行卡。

7.2 支付保护中心

ColorOS 支付保护中心对为支付应用提供安全的支付环境隔离空间，并对支付环境进行全面检测，确保支付环境安全。启用支付保护中心后，系统会在支付类 App 前台运行时

检查运行环境，一旦发现安全隐患，立即进行风险展示并对用户进行修复提醒。

支付环境隔离：

- 应用隔离：屏蔽相关接口，防止恶意应用感知到支付类应用。
- 支付环境隔离：如果支付应用在后台运行超过 1 分钟，则结束进程。

运行环境检测：

- 系统安全环境检测：检测设备是否 root、安全补丁是否安装、默认短信应用是否为受信任的应用、是否允许 USB 传输数据。
- WLAN 安全检测：如果连接 WLAN，则检测 WLAN 是否加密、是否为虚假 WLAN、是否有 DNS 劫持、是否被 ARP 攻击。（参见"Wi-Fi 安全检测"节）
- 应用安全检测：查看病毒扫描的结果。病毒扫描发生在用户手动触发及应用安装等时机。

7.3 短信验证码保护

短信验证码已经成为可信操作的重要验证因子，一旦泄露可能导致用户严重财产损失及重要信息泄露。很多第三方应用在安装时申请短信读取权限，用户授权后，很少关注或调整对应权限，导致第三方应用可随时读取短信中的重要或敏感信息。

ColorOS 提供验证码保护功能，以有效降低验证码泄露地风险。当 ColorOS 接收到短信时，短信应用对该短信进行智能解析，如果判断为验证码，将禁止所有第三方应用读取，避免由于短信读取权限误授权给恶意应用，导致验证码泄露地风险。

8 设备管理

为应对用户丢失手机、老人丢失及诈骗和儿童沉迷手机等场景，ColorOS 提供查找手机功能、远程守护、儿童空间等设备管理功能。

8.1 查找手机

考虑到用户丢失手机时需找回手机及防止隐私数据泄露，ColorOS 提供查找手机、激活锁、抹除数据的功能。手机联网的前提下，开启"查找手机"功能后，当前手机设备会与已登陆的 HeyTap 账号形成绑定关系。如果手机丢失，用户可登陆云服务网页 cloud.heytap.com 或用使用其他 OPPO 手机的登录"查找手机"功能对丢失的设备进行定位、响铃、锁定和抹除数据操作。

此外，ColorOS 提供了设备激活锁功能。此功能在启用查找手机功能后会同步开启。若手机丢失并被强制清除数据，手机重启后需要使用清除数据前的原 HeyTap 账号重新认证机主身份后，方可使用。

*注：上述功能仅适用于在中国销售的 OPPO 手机。对于在其他国家销售的 OPPO 手机，您可参见由 Google 提供的"查找我的设备（Find My Device）"功能。

8.2 远程守护

如果您和您的家人都使用 OPPO 手机，则可使用"远程守护"功能将两台手机绑定为家人状态。您可随时查看家人的实时位置，为家人添加特定的"守护区域"，当家人的位置超出此区域时，您将会收到提醒。您可以查看家人的应用使用时间，并为其设置限制。在家人

的手机上出现诈骗电话、手机病毒及支付安全风险时，您会收到提醒，并可远程将家人收到的诈骗电话加入黑名单。

*注：该功能仅限在中国销售的 OPPO 手机。对于其他国家销售的 OPPO 手机，您可参见由 Google 提供的"数字健康与家长控制（Digital Wellbeing & Parental Controls）"功能。

8.3 儿童空间

为防止儿童沉迷手机或误操作致话费损失等，ColorOS 提供"儿童空间"功能。设定时间并启动"儿童空间"后，设备当中的应用中将只能使用用户指定的应用。用户也可选择关闭或开启儿童空间中的移动网络。

9 数据安全

本章节介绍 ColorOS 的数据安全防护机制。ColorOS 文件系统分为系统分区和用户分区。系统分区只读且与用户分区隔离，普通应用无权限访问；对存储在用户分区的数据，系统提供基于文件的数据加密和目录权限管理机制，限制不同应用间的数据访问。同时，针对用户分区，ColorOS 提供包括安全存储、可信 UI、密钥管理、FBE、数据擦除、锁屏密码保护、指纹保护、安全键盘、密码本等从硬件、系统、应用提供整体的数据保护机制。

9.1 安全存储

ColorOS 基于 TEE 提供安全存储能力，将数据加密存储在安全存储器中，并对数据访问进行严格管控，防止数据非法访问。ColorOS 提供以下安全存储实现机制：

1）安全文件系统（Secure File System，SFS）

TEE 中运行的可信应用（Trusted Application, TA）通过 SFS 接口加密并存储密钥、证书、指纹模板等敏感信息，加密密钥由设备唯一密钥（HUK）和可信应用 Id 等信息在 TEE 下进行派生，并始终在设备 TEE 内，经过加密的数据只有 TA 可以访问。

2）重放保护内存块（Replay Protected Memory Block，RPMB）

RPMB 是 eMMC 中具有安全特性的分区，通过提供防重放和认证保护，防止存储在 RPMB 中的密钥、证书等敏感信息被恶意篡改、删除。RPMB 安全性较 SFS 更高。

数据进行加密存储，加密密钥由设备唯一密钥（HUK）等信息在 TEE 下进行派生。使用 RPMB 前需要在安全环境下进行 key provision，将 Authentication Key 预置到

eMMC 中，这把 key 参与 MAC（消息认证码）计算。写数据时 Counter 参与 MAC 计算，用于防重放攻击，读数据时 Nonce（随机数）参与 MAC 计算，用于数据认证。

3）一次性可编程存储器（One Time Programmable, OTP）

OTP 是一块特殊的存储区域，该区域基于熔丝位烧断的硬件原理，可以被多次读取，但仅可被烧写一次，用于存储设备唯一密钥（HUK）,安全启动信任链根公钥 hash 等敏感信息。OTP 仅允许在 TEE 中访问，没有对外提供导出接口。

4）安全单元（Secure Element, SE）

ColorOS 安全元件是防物理攻击的电子元件，用于密钥和数字证书等敏感数据的存储和密码运算。TEE 提供 SE 访问的基础服务，仅对可信应用提供调用接口。

9.2 可信 UI

可信 UI 是指在关键信息的显示和输入时，屏幕显示和键盘等硬件资源由 TEE 控制和访问，系统中的软件不能访问。可信 UI 可在排除干扰的情况下，为用户和应用之间提供安全通道，抵御输入法劫持、钓鱼、恶意截屏等方式对用户重要数据（如密码、PIN 码、信用卡账号、手机号、邮件等）的窃取。

9.3 密钥管理

ColorOS 支持 Keystore 特性对应用所使用的密钥和证书的全生命周期进行管理，密钥管理具有如下功能：

1）密钥生成和存储

支持硬件加解密引擎，TEE 根据应用指定的密钥生成算法生成对称密钥和非对称密钥，生成的密钥由 TEE 维护的密钥加密密钥经过加密后做存储。

2）密钥导入和导出

业务密钥和其他需要外部生成的密钥通过安全的方式导入到 TEE 的安全存储区域，并用密钥加密密钥进行保护；根据业务需求，可以导出非对称密钥公钥，完成对此私钥签名数据的验证功能。

3）加解密服务

加解密服务提供密码算法接口，可信应用通过该服务接口执行密码运算，密码运算在 TEE 中运行。

4）密钥销毁

可信应用运行时产生的密钥数据，在生命周期结束后进行销毁。

5）密钥认证

OPPO 手机在生产时在设备中注入了由 Google 公司颁发的证书，目的是确保设备是可信的，生成的密钥都可以使用 Google 的证书进行校验。在线认证时，密钥认证功能可以对 ColorOS 设备进行认证。

除了对应用所使用的密钥和证书的全生命周期管理功能外，Keystore 还增加了密钥提取防范和身份验证等安全功能，避免在 Android 设备之外以未经授权的方式使用密钥。

1）密钥提取防范

为防止攻击者在 ColorOS 设备之外提取密钥，ColorOS 通过 Keystore 密钥执行加密操作时，应用会将待签署或验证的明文、密文和消息发送到执行加密操作的系统进程，而不是应用进程。因此，即使应用进程遭受攻击，攻击者也无法提取密钥材料。同时，ColorOS 将密钥绑定至 OPPO 设备的 TEE 的安全硬件中，使密钥永远不会暴露于安全硬件之外。即使 ColorOS 操作系统遭受攻击或者攻击者读取到设备的存储空间，也无法从设备上提取这些绑定安全硬件的密钥材料。

2）密钥使用授权

为避免在 ColorOS 设备上以未经授权的方式使用密钥，在生成或导入密钥时，Keystore 会让应用指定密钥的授权使用方式。一旦生成或导入密钥，其授权将无法更改。以后每次使用密钥时，都会由 Keystore 强制执行授权。ColorOS 支持的密钥使用授权分为以下几类：

- 加密：授权密钥算法、运算或目的（加密、解密、签署、验证）、填充方案、分块模式以及可与 密钥搭配使用的摘要；
- 时间有效性间隔：密钥获得使用授权的时间间隔；
- 用户身份验证：密钥只能在用户最近进行身份验证时使用。

9.4 文件系统加密（FBE）

ColorOS 支持 Android 的文件级加密（File-Based Encryption，FBE）功能特性。FBE 可使用不同密钥对不同文件进行加密，并且可以对文件进行单独解密。在启用了 FBE

的设备上，用户有两个可供应用使用的存储位置：

- 凭据加密 （CE） 存储空间：默认存储位置，只在用户解锁设备后才可用；
- 设备加密 （DE） 存储空间：在直接启动模式期间以及用户解锁设备后均可用。

ColorOS 使用凭据加密 （CE） 存储空间作为默认存储位置，保证应用和数据在用户认证通过后才能使用；同时将闹钟、铃声、短信、无线等应用数据保存在设备加密 （DE） 存储空间，这些应用能够在设备通电但用户尚未解锁设备时访问数据，利用系统能保护私密用户信息。

9.5 数据擦除

ColorOS 用户使用"彻底清除全部数据"操作时，不仅删除用户数据的逻辑地址，还会通过对物理存储器进行全 0 或全 1 覆写，彻底清除物理地址空间中的数据，确保数据无法被软硬件手段恢复，保障用户设备在转售、废弃后的数据安全。

用户可以在 设置〉其他设置〉还原手机>彻底清除全部数据 中彻底删除所有个人数据，包括应用数据（/data/data、/data/user 下的数据）、用户数据图片（/sdcard/下的数据）等。

9.6 锁屏密码保护

ColorOS 支持三种锁屏密码：绘制图案、数字密码和字母数字混合密码。

锁屏密码通过设备唯一密钥 HUK 保护，在 TEE 中进行加密。在用户创建、修改锁屏密码，或验证锁屏密码进行解锁时，这些密码的处理都在 TEE 环境中进行

锁屏密码的解锁认证操作在 TEE 中进行。ColorOS 对锁屏密码输入错误次数进行了限制，防止锁屏密码被暴力破解。连续输错 5 次锁屏密码，手机锁定将 30 秒，此后每输错 1 次密码，手机都将锁定 30 秒。

设置锁屏密码的方法是通过设置>指纹、面部与密码〉锁屏密码。建议用户使用较复杂、较长的密码，防止密码因过弱而被破解。

9.7 指纹保护

ColorOS 设备的指纹识别功能，要求用户的指纹采集、注册、识别和认证都在 TEE 内部进行，保证指纹数据安全，其中对指纹图像的处理过程（预处理，特征提取，录入及认证）均在 TEE 内完成，指纹相关数据不会被传出 TEE 区域外。外部的应用无法获取指纹数据，仅能通过框架的接口进行认证和获取认证结果。如下图所示用户可以注册一个或多个指纹，并使用这些指纹来解锁设备以及执行其他任务。ColorOS 会利用 Fingerprint HIDL（硬件接口定义语言）连接到供应商专用库和指纹硬件（例如指纹传感器）。FingerprintService 和 fingerprintd 会通过 Fingerprint HAL 调用供应商专用库，以便注册指纹以及执行其他操作，TEE 中 Keystore API 和 Keymaster 组件提供由硬件支持的加密功能，以便在 TEE 中安全地存储密钥。

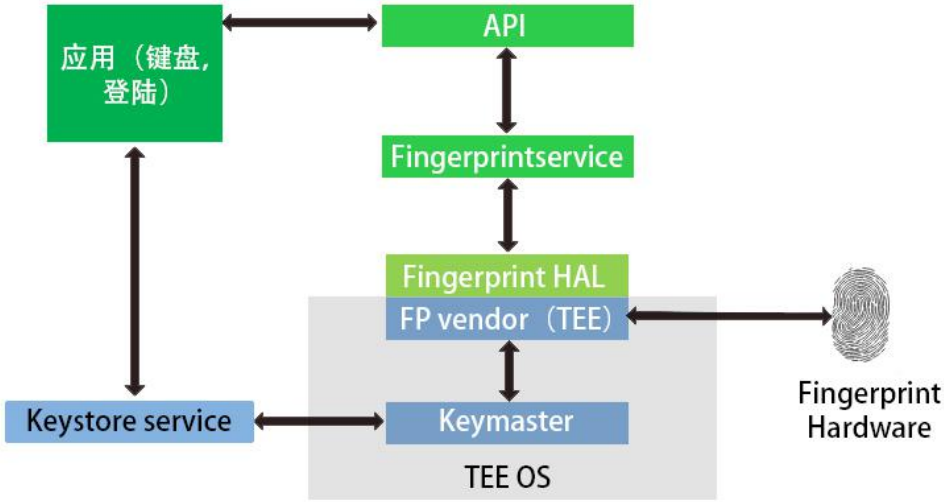

图 9-7 指纹安全原理

9.8 安全键盘

安全键盘旨在对用户的密码输入形成保护，避免用户的密码信息泄露。启用安全键盘功能后，当系统检测到输入为密码类型时，自动调起 OPPO 安全键盘（银行、支付类应用优先使用应用自有键盘），系统在安全键盘调起时禁止任何应用（包括系统应用和第三方应用）进行截屏和录屏操作。安全键盘无任何联想及记忆功能，没有联网权限，不会收集用户的密码数据。

9.9 密码本

ColorOS 提供密码本功能，旨在提升用户对当前手机众多应用的账号、密码维护效率，降低账号或密码被遗忘风险。功能开启后，App 上首次输入账号密码时，密码本对用户的账号、密码进行集中保存。同时密码本可以与人脸识别、指纹识别和锁屏密码关联，在用

户登录应用时自动填充登录信息，方便用户进行密码管理。

存储在密码本中的用户密码使用 AES256 位加密算法进行加密，密钥保存在 TEE 中，保障用户的隐私数据安全。

存储在密码本中用户密码密文实时同步到云端，以帮助用户实现登录同一 OPPO 账号的多台手机间的密码数据多端协同。

10隐私控制

本章节主要阐述对用户的隐私控制机制。OPPO 设备中存在用户的隐私，如：联系人、短信、照片等。为了保护用户的隐私，ColorOS 确保预置的应用完全符合国家法律法规和行业主管部门对个人信息隐私合规的各项要求，同时提供对应用的权限管理、保护个人信息、录音/录像提醒、位置服务、应用锁、私密保险箱隐私控制扩展功能。

10.1 系统分身

随着社会的高速发展，人们的工作节奏越来越快，商务人群希望在上班时高效率工作，下班后快速进入生活状态，现有的多用户切换效率不高，主/子用户间无法交互，不符合工作生活双系统的需求，无法满足人们隐私保护高需求。

系统分身基于多用户技术开发，用户可在锁屏通过密码或指纹快速在双系统间切换，同时双系统间支持数据导入导出、通知共享、在主系统隐藏系统分身入口。可满足将工作/生活/娱乐应用隔离使用，无痕隐藏私密数据，快速在双系统间切换的需求。

10.2权限管理

Android 的权限管理要求应用程序安装时需提示所需的权限，并经过用户同意授权才能安装，以限制应用程序对敏感的接口和资源的访问。

ColorOS 继承了 Android 的权限管理机制并进行扩展增强,允许用户对已安装的应用程序所申请的权限进行细粒度的控制。用户可以在设置 > 应用管理 > 应用权限 菜单查看已安装的 App 申请的权限集或者某项权限被申请的 App 清单， 管理某个应用拥有的所有权限，可以对权限进行单独允许或禁止，也可以管理某项权限允许哪些应用拥有或关闭。

ColorOS 提供权限使用记录功能，对手机上非系统应用最近 30 天的权限使用行为进行详细记录，包括应用名称、允许状态、调用时间。支持以全部记录、权限、应用三个维度查看，并可筛选已允许、已禁止的权限使用记录。基于权限使用记录功能，用户可追溯窃取隐私的应用以及对三方应用肆意使用用户权限形成威慑。

该功能解决了应用获取权限后随时调用而用户无感知的问题，避免三方应用在用户不知情的情况下窃听、偷拍、跟踪用户。对三方应用的流氓行为形成威慑，保障用户隐私。

位置、相机、麦克风权限支持"仅本次允许"授权，避免应用获得权限后，在用户未使用应用期间，窃取用户隐私数据。"仅限本次允许"权限在应用退出或回到后台一定时间后，系统自动回收相应权限，应用需要使用时需再次向用户申请

*注：此功能仅限在中国大陆销售的手机。

10.3保护个人信息

针对某些应用必须读取通话记录、通讯录、信息、日程信息等个人信息才可使用的情

况，ColorOS 为用户提供保护个人信息功能。开启后即使应用已获得相应权限，仍无法获得上述信息的真实内容，解决了部分应用不给权限不允许使用的问题，该功能既不影响应用的正常使用，又能避免真实信息泄露。

用户可通过 ColorOS 彻底删除全部个人信息，确保个人信息无法被软硬件手段恢复，保障用户设备在转售、废弃后的数据安全。具体方法可参见 9.5。

*注：此功能需要依赖"oppo 通信应用（拨号盘、联系人）"若无集成则无此功能。

10.4隐私行为提醒

ColorOS 对敏感权限使用进行提示。当非系统级应用在使用相机、麦克风、地理位置权限时，状态栏右侧会立即出现对应权限的调用状态图标。用户通过下拉状态栏，在通知中心点击敏感权限图标可在弹框中查看正在使用敏感权限的所有应用信息。用户可在弹框中直接点击应用快速跳转到的权限管理页对该应用进行权限管理，也可通过"查看详情"选项跳转到权限使用记录页，获取更详细的权限使用情况。

10.5位置服务

为保护用户位置隐私信息，ColorOS 提供 GPS、WLAN 和移动基站的位置服务关闭功能。选择关闭位置服务后，将同时关闭 GPS / WLAN / 移动基站信息的三种定位功能，彻底关闭用户的位置信息，保护用户的隐私安全。

用户可以在设置>其他设置>设备与隐私>位置信息选项中开启或关闭位置信息，或者在下拉菜单状态栏中快捷管理位置信息。此外，用户可以查看最近请求位置信息的应用。

10.6应用锁&应用隐藏

为了防止用户将手机借出时，他人未经允许访问涉及隐私的应用，ColorOS 提供了“应用锁”机制。用户可以为应用软件设置访问密码、指纹、人脸验证保护，必须通过验证才能允许访问被“应用锁”保护的应用，有效保护用户的隐私。

同时 ColorOS 提供应用隐藏功能，用户可以通过此功能隐藏应用的图标，保护私密应用。

10.7私密保险箱

ColorOS 私密保险箱提供基于用户密码加密的保护空间。用户可以将一些敏感或重要的个人文件（照片、音频、视频、文档等）添加到私密保险箱中进行加密保护。

用户可以通过设置隐私密码可开启该功能，目前私密保险箱支持密码、指纹、人脸认证方式，只有通过验证的用户才能打开私密保险箱。

私密保险箱的隐私密码储存于芯片级安全空间，防止密码被窃取。

11 术语表

英文缩写	英文全称	中文全称
AES	Advanced Encryption Standard	高级加密标准
API	Application Programming Interface	应用程序接口
APK	Android application package	Android 应用程序包
ARP	Address Resolution Protocol	地址解析协议
ASLR	Address space layout randomization	地址空间配置随机加载
AVB	Android Verified Boot	安卓启动验证
BL	Bootloader	引导程序
CE	Credential Encrypted	凭据加密
CVV	Card Verification Value	信用卡验证值
DE	Device Encrypted	设备加密
DEP	Data Execution Prevention	数据执行保护
DNS	Domain Name System	域名系统
eMMC	Embedded Multi Media Card	嵌入式多媒体存储卡
FBE	File-Based Encryption	文件级加密
Fuse	Filesystem in Userspace	用户空间文件系统
GPS	Global Positioning System	全球定位系统
HUK	Hardware Unique Key	硬件唯一密钥
IMEI	International Mobile Equipment Identity	国际移动设备识别码
IP	Internet Protocol	网际互连协议
IPSec	IP Security	IPSec 安全协议
JCP	Java Card Platform	Java Card 平台
JTAG	Joint Test Action Group	联合测试工作组

KASLR	Kernel address space layout randomization	内核地址空间布局随机化
L2TP	Layer Two Tunneling Protocol	第 2 层隧道协议
MAC	Message Authentication Code	消息认证码（带密钥的 Hash 函数）
MAC	Mandatory Access Control	强制访问控制
MPPE	Microsoft Point-to-Point Encryption	微软点对点加密术
NFC	Near Field Communication	近距离无线通信
OTA	Over the Air	空中升级
OTP	One Time Programmable	一次性可编程存储
PAN	Privileged Access Never	特权模式访问禁止
PIN	Personal identification number	个人身份识别码
PPP	Point to Point Protocol	点对点协议
PPTP	Point-to-Point Tunneling Protocol	点到点隧道协议
PSK	Pre-Shared Key	预共享密钥
PXN	Privileged Execute Never	特权模式执行禁止
REE	Rich Execution Environment	富执行环境
RPMB	Replay Protected Memory Block	重放保护内存块
RSA	Rivest Shamir Adleman	公开密钥密码体制
SE	Secure Element	安全单元
SELinux	Secure Enhanced Linux	安全增强 Linux
SFS	Secure File System	安全文件系统
SoC	System on Chip	系统级芯片
SSL	Security Socket Layer	安全套接字协议
TA	Trusted Application	可信应用
TEE	Trusted Execution Environment	可信执行环境

TLS	Transport Layer Security	传输层安全协议
UI	User Interface	用户界面
UID	User Identify	用户 ID
USB	Universal Serial Bus	通用串行总线
VPN	Virtual Private Network	虚拟专用网
WAPI	WLAN Authentication and Privacy Infrastructure	无线局域网鉴别和保密基础结构
WEP	Wired Equivalent Privacy	有线等效加密
WLAN	Wireless Local Area Network	无线局域网
WPA	Wi-Fi Protected Access	Wi-Fi 保护访问