PlugOS 安全白皮书

版本：V1.1

声明

本文档的内容会不定期进行更新。

本文档仅作为使用指导，文档中的所有陈述、信息和建议，均不形成任何明确或隐含的保证。

目 录

1. 前言

1.1. 摘要

随着数据安全事件频发和全球隐私保护意识的提高，移动与个人计算设备的安全性成为信息社会的核心问题。用户既担心黑客入侵、恶意应用窃取数据，也担心在胁迫检查、设备丢失等场景下隐私被暴露。传统手机等移动终端往往以功能和商业化为导向，难以保障公民的数据主权。

PlugOS 作为一款运行在独立便携硬件中的安全操作系统，以隐私优先、零信任、最小化可信边界为核心设计理念，构建了覆盖硬件、内核、系统与应用的多层次防御架构。本白皮书通过公开 PlugOS 的认证合规、安全威胁模型、安全与隐私架构、安全管理等，为技术专家、安全管理者、决策者及所有关注数字权利的用户提供一个透明、可验证、可审计的视角，回答最关键的问题：为什么 PlugOS 值得用户合理地信任。

1.2. 引言

1.2.1. 背景：日益严峻的隐私与安全挑战

在高度互联的数字时代，个人数据已从信息载体升级为驱动商业决策与技术迭代的核心资产，小到日常消费记录、位置轨迹，大到生物识别信息、金融账户数据，均承载着用户核心权益。主流操作系统普遍存在数据优先倾向，为追求商业价值，常默认开启多维度数据收集,通过系统权限获取应用使用时长、设备硬件信息等，甚至在用户未明确授权时，将碎片化数据整合为用户画像，用于精准广告、产品推荐或第三方共享。这种被动采集模式模糊了隐私边界，数据流转链路失控，部分数据可能流向境外服务器或未授权机构，用户既不知数据用途，也难撤回授权，隐私自主权被严重削弱。

同时，用户数据主权面临多场景、高隐蔽、强破坏性的复合威胁。网络层面，移动设备攻击手段升级，黑客伪造系统更新包、利用漏洞植入恶意代码窃取加密数据，钓鱼攻击通过伪装诱导泄露敏感信息，2024 年全球移动钓鱼事件同比增 37%，近六成针对金融、医疗高价值数据；物理层面，设备盗窃、定向攻击频发，不法分子拆解硬件提取未加密数据，供应链漏洞导致设备出厂即被监控，已影响超千万台终端。

此外，人身胁迫与社会工程学攻击成为隐形威胁，用户或因胁迫提供解锁密码、生物信

息，社会工程学攻击则利用心理弱点突破防线。这些威胁交织，致使用户数据泄露、财产损失，甚至引发身份盗用、名誉损害，凸显构建高安全、强隐私保护体系的迫切性。

1.2.2. PlugOS：重塑数字主权

PlugOS 的诞生正是为了应对上述挑战。它并非在现有系统上进行增量式的安全修补，而是从第一性原理出发，重构了一个以安全和隐私为基石的计算平台。PlugOS 将完整的智能系统运行环境、核心应用及用户数据封装于一个独立的便携式硬件中，通过加密信道与用户主机设备进行屏幕、键盘、网络等 I/O 交互，从而创建了一个可验证、可管控、与宿主环境严格物理隔离的可信计算环境。PlugOS 打破主流操作系统的数据收集惯性，通过硬件 - 内核 - 系统 - 应用全层级深度防御架构，将隐私安全设计嵌入每一个技术环节，既抵御外部攻击风险，更从根源上保障用户对个人数据的知情权、控制权、删除权，让操作系统真正成为用户数据安全的守护者，而非数据流转的商业中转站。

1.2.3. 白皮书目的与目标读者

本白皮书旨在为技术专家、安全管理人员、决策者及注重安全和隐私的个人用户提供一份详尽的技术性说明，将透明地展示 PlugOS 的架构与机制如何应对现代数字世界中的各类安全挑战。

由于本文深度探讨系统安全、密码学及硬件安全等专业领域，我们假设读者已具备一定的信息安全基础知识。

1.3. 术语和定义

下列术语和定义适用于本文档。

术语	缩写	定义
宿主机/宿主设备	Host Device	指 PlugOS 插入后提供电力和外设能力（如屏幕、键盘、触控、网络）的设备，可以是智能手机、平板或计算机。
宿主机应用，或宿主机客户端	Host App / Companion App	安装在宿主机上的官方应用程序，是 PlugOS 与宿主机交互的核心桥梁。主要功能包括：转

		发宿主机外设能力、加密传输 PlugOS 输出、状态监控与管理。
产品密钥	Product Key	每台 PlugOS 出厂时写入的唯一序列号与加密凭证，用于设备激活以及与宿主机的安全绑定。
安全绑定	Secure Binding	PlugOS 与宿主机首次配对时的双向认证过程，通过密码校验与动态令牌实现设备与宿主机的一一绑定，防止未经授权的宿主机访问。
可信执行环境	Trusted Execution Environment (TEE)	在计算平台上通过硬件隔离构建的安全区域，保障代码和数据的机密性与完整性。TEE 用于在独立环境内执行敏感任务，如隐私认证和数据保护。
独立安全芯片	Secure Element (SE)	一个物理上独立的、具备高度防篡改能力的专用微处理器，专为存储和处理最高级别的机密信息（如加密密钥）而设计。
硬件信任根	Hardware Root of Trust, HRoT	一个在硬件制造过程中就已建立、且后续无法被软件修改的信任基础。它是整个系统安全启动和加密操作的起点。
零信任架构	Zero Trust Architecture	一种安全模型，核心原则是“从不信任，始终验证”，对任何访问资源的请求都进行严格的身份验证和授权，默认不信任宿主机及其 App。
攻击面	Attack Surface	系统中所有可能被攻击者利用来发起攻击的入口点的总和。攻击面越小，系统通常越安全。
端到端加密	End-to-End Encryption, E2EE	一种通信加密方案，确保数据在从发送端到接收端的整个传输过程中始终为密文，只有通信

		双方能够解密。
设备指纹	Device Fingerprinting	通过收集设备的多种软硬件特征来创建一个能唯一标识该设备的“指纹”的技术，常被用于追踪用户。
传感器虚拟化	Sensor Virtualization	在系统底层拦截应用对硬件传感器的访问，并向其提供由用户控制的虚拟数据，以此对抗设备指纹追踪。
胁迫密码	Duress Password / Duress Code	一种应对物理胁迫场景的安全机制，输入此密码会销毁数据或进入一个不含真实数据的“伪装系统”。
数据自毁	Data Self-Destruction	系统在满足预设条件（如用户触发、检测到恶意攻击、胁迫场景）时，自动删除所有敏感数据（如用户文件、密钥、应用数据），且删除后无任何残留，无法通过技术手段恢复。硬件自毁条件下可能使得设备不再能正常使用。
供应链攻击	Supply Chain Attack	攻击者不直接攻击最终用户，而是攻击产品在设计、生产、分发等供应链环节中的薄弱点，从而植入恶意代码。
通用准则评估保证级别	Common Criteria, CC EAL	一套国际公认的信息技术产品安全评估标准，EAL 级别越高，代表产品的安全保证程度越高。
数据最小化	Data Minimization	隐私保护的基本原则之一，要求系统和组织仅收集、使用完成业务目标所必需的最少个人信息。

2. 安全责任

在应对当前日益严峻的隐私与安全挑战过程中，PlugOS 与客户需明确各自安全责任，构

建技术保障 + 用户规范的协同安全体系，双方协同应对多维度安全挑战，共同守护数据主权与隐私安全。

2.1. PlugOS 的安全责任

PlugOS 在设计与运营过程中，承担核心的技术与合规安全责任，确保系统本身是可信赖的“安全基座”，具体包括：

- **技术架构安全**
  - **物理与逻辑隔离**：PlugOS 独立于宿主系统，硬件上具备独立计算与存储能力，避免与宿主机的数据混淆。
  - **硬件级防护**：通过 TEE、SE 等可信组件实现执行与密钥保护；支持高强度加密、哈希校验，确保机密性与完整性。
  - **抗强制攻击**：内置暴力破解清除、胁迫密码自毁等机制，防范物理盗窃与人身胁迫导致的数据泄露。
- **提供数据与隐私保护**
  - 默认最小化数据收集，无广告、无推送、不监听。
  - 数据本地存储与计算，避免隐形上传及跨境数据流转风险。
- **安全运营与合规**
  - 建立漏洞监测与响应机制，实施定期更新与补丁修复。
  - 推行漏洞奖励计划，与社区和合作伙伴共同提升安全性。
  - 确保系统设计与国际/国内安全合规标准（如 GDPR、PIPL、ISO/IEC 27001）保持一致。
- **客户支持与应急响应**
  - 提供安全技术支持与指导。
  - 当客户遭遇突发事件（如设备丢失、可疑入侵），可快速协助隔离风险并恢复安全状态。

2.2. 客户的安全责任

客户作为 PlugOS 的最终使用者，在设备管理和使用环节扮演着至关重要的角色。客户的

安全意识和规范操作是实现安全效果最大化的关键。客户的核心安全职责包括：

- **账户与设备凭证妥善管理**：妥善保管设备解锁密码、产品密钥等关键凭证，不向任何第三方泄露账户信息。建议使用高强度密码以提升账户安全。
- **谨慎的权限管理与应用授权**：根据实际需求合理配置系统权限，不随意授权第三方应用访问敏感数据（如位置、通讯录），从源头减少社会工程学攻击的潜在风险。
- **环境警觉与操作规范**：在使用 PlugOS 处理敏感信息时，需对所处物理环境保持高度警觉，检查周围是否存在隐藏的监控装置（如摄像头、录音设备）。同时，避免在人员流动复杂、易被窥视的公共区域（如开放式办公区、公共交通）进行敏感操作。
- **设备物理安全保障**：尽管 PlugOS 具备硬件级防篡改能力，但客户仍需妥善保管设备本身，防止设备遗失，避免攻击者通过物理接触或诱导操作等方式间接获取信息。
- **保持系统更新与及时响应**：关注 PlugOS 推送的安全提示与更新通知，及时完成系统升级，确保设备始终运行在最新的安全版本上。在发生设备丢失、疑似数据泄露等异常情况时，第一时间联系 PlugOS 技术团队，启动应急响应流程，将风险扩散降至最低。

3. 安全认证与合规

在安全与合规问题上，PlugOS 不仅依赖自我承诺，更以**“国际权威认证、全球法规对齐、行业标准参与”**三重保障，构建出可被最严苛用户信赖的安全基准。我们坚持“外部独立验证 + 内部持续改进”的合规理念，确保 PlugOS 在全球范围内的长期可信。本章节将介绍我们所获得的各项认证、遵循的法律法规以及参与的行业标准。

3.1. 国际体系认证

我们的研发与管理体系严格遵循国际权威标准，从需求分析、架构设计到开发测试的每一个环节都嵌入了严谨的安全考量。我们已获得多项第三方权威认证，包括 ISO/IEC 9001:2015、ISO/IEC 27001:2022、ISO/IEC 27701:2019、ISO/IEC 29151:2017、CMMI 三级等等，这充分证明 PlugOS 在信息安全、隐私保护和软件工程管理方面具备成熟、规范且可持续的能力，为 PlugOS 的卓越安全性能奠定坚实根基。

3.1.1. ISO/IEC 9001（质量管理体系认证）

ISO/IEC 9001 是由国际标准化组织（ISO）与国际电工委员会（IEC）联合发布的全球通用质量管理体系标准，核心聚焦以顾客为关注焦点、过程方法、持续改进三大理念，为组织提供系统化的质量管理框架，确保产品 / 服务在全生命周期内稳定满足顾客需求与法规要求。

ISO/IEC 9001 是 PlugOS 质量管理的基石，通过将标准要求融入研发、生产、交付、服务全流程，PlugOS 实现了安全功能稳定、产品体验一致、用户需求响应高效的目标，为用户兼具安全性与高质量的操作系统解决方案。

3.1.2. ISO/IEC 27001（信息安全管理体系认证）

信息安全管理体系标准(ISO27001)由国际标准化组织（ISO）和国际电工委员会（IEC）联合制定，是全球广泛认可的信息安全管理领域的权威标准。ISO27001 在保护信息资源、推动信息化健康发展方面有着不可替代的作用可有效保护信息资源，保护信息化进程健康、有序、可持续发展。

ISO27001 明确了信息安全管理的各项要求和最佳实践，为 PlugOS 的研发管理提供了安全保障框架，从项目规划阶段就将信息安全纳入考量，确保各个环节都符合安全标准，帮助组织满足信息安全的合规要求，避免因违规而面临的法律风险和声誉损失。

3.1.3. ISO/IEC 27701（隐私信息管理体系认证）

ISO/IEC 27701 是由国际标准化组织（ISO）和国际电工委员会（IEC）共同制定的国际标准，是对 ISO/IEC 27001 信息安全管理体系标准的扩展，专注于隐私信息管理，为组织在个人信息保护方面提供了一套系统化、可操作的框架，并且其要求与全球主流隐私法规（中国 PIPL、欧盟 GDPR、美国 CCPA/CPRA、巴西 LGPD 等）深度对齐。

我们依据 ISO/IEC 27701 梳理了 PlugOS 的个人信息全生命周期管理流程，建立了标准化隐私风险防控机制，消除了管理盲区并持续优化。

3.1.4. ISO/IEC 29151（个人可识别信息保护管理体系）

ISO/IEC 29151 是国际标准化组织（ISO）和国际电工委员会（IEC）联合发布的一项关于个人身份信息保护的国际标准，聚焦于个人身份信息处理者在处理个人身份信息时应遵循的行为准则，旨在增强对个人身份信息的保护，从而维护公众的隐私权益，在全球数字化进程中发挥着重要作用。

PlugOS 严格执行该标准，规范个人信息在收集、存储、处理、使用和披露等环节的操作，从根本上维护用户的隐私权益。

3.1.5. CMMI 三级认证（能力成熟度模型三级认证）

CMMI（Capability Maturity Model Integration，能力成熟度模型集成）是全球公认的衡量组织项目管理、工程开发及流程管理能力的权威标准。其中，CMMI 三级（已管理级，Managed Level）是组织从被动应对转向主动管控的关键里程碑，标志着组织的核心业务流程已实现标准化、规范化，并能基于流程稳定交付高质量成果。

PlugOS 的研发设计全程以 CMMI 为核心框架，对标 CMMI 已定义级的流程标准化、执行规范化、资产可复用要求，将 CMMI 的管理理念嵌入 PlugOS 的需求分析、架构设计、开发测试、交付运维全生命周期，从根源上保障产品的安全性、稳定性与可扩展性，为用户提供 高可靠、低风险的安全操作系统体验。

3.2. 产品安全认证

PlugOS 的安全性建立在经过业界最严格标准验证的硬件组件之上，其硬件组件现已通过 CC（Common Criteria）认证体系。CC（Common Criteria for Information Technology Security Evaluation，信息技术安全评估通用准则）认证体系，是目前全球范围内最权威、最通用的信息安全产品与系统评估标准，实现不同国家和地区间的安全评估结果互认，为企业、机构选择安全产品提供可靠依据。

3.2.1. TEE OS 安全认证

PlugOS 内置的 TEE OS，作为守护系统安全的关键防线，已成功通过 CC EAL 4+ 级别的安全认证，不仅证明其具备抵御常规攻击的能力，更体现了其在大规模商用场景中的安全可靠性，是我们技术实力与用户安全体验的重要保障。

同时，这款 TEE OS 还经过了十亿级产品的量产验证。十亿级产品的量产实践，不仅验证了 TEE OS 在技术层面的可靠性，更证明了其在大规模商业应用中的可行性与稳定性，用户在使用 PlugOS 时，对其安全性能充满信心 。

3.2.2. SE 安全认证

PlugOS 所选用的独立安全芯片（SE）组件凭借其卓越的安全功能，为用户构建起一道坚不可摧的安全屏障。该芯片已斩获 CC EAL 6+ 级别的安全认证，在全球安全标准体系中处于高阶地位，为各类应用场景筑牢安全根基。

CC EAL6 + 认证确保该芯片组件能在复杂金融环境中稳定运行。无论是 PlugOS 用于银行核心交易，还是守护用户支付密码、交易记录等敏感信息，都能提供可靠的安全保障，让用户在享受数字化金融服务时无后顾之忧 。

3.3. 全球法律法规对齐

PlugOS 践行“**设计即隐私**”和“**数据最小化**”原则，我们不收集、不处理、不存储任何用户可识别数据。这一架构设计，使其天然符合全球主流数据保护法规的核心要求，如中国的《中华人民共和国个人信息保护法》(PIPL)、欧盟的《通用数据保护条例》(GDPR)、美国的《加州消费者隐私法》(CCPA) 等。

3.3.1. 《中华人民共和国个人信息保护法》(PIPL)

PIPL 是中国首部为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利

用，根据宪法制定的法规。该法明确规定，自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。 在中国境内处理自然人个人信息的活动均受其约束。

PlugOS 的设计与功能完全契合该法的要求。从设计理念来看，PlugOS 秉持设计即隐私的原则，坚决拒绝数据采集与行为分析，系统无广告、无推荐、不监听、不上传，充分尊重个人对自身信息的控制权，完全符合《中华人民共和国个人信息保护法》中对个人信息处理者应遵循合法、正当、诚信原则的规定。

3.3.2. 《通用数据保护条例》(GDPR)

《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）是欧盟极具影响力的数据保护法规。该条例不仅对欧盟境内组织影响深远，全球范围内只要涉及欧盟个人数据处理的企业，都必须调整数据管理策略以合规。GDPR 在全球数据保护领域树立了标杆，极大程度上改变了企业处理个人数据的方式，有力推动个人数据保护迈向新高度。

PlugOS 全面遵循《通用数据保护条例》（GDPR）严格要求，我们秉持设计即隐私理念，杜绝数据采集与行为分析，其独立安全芯片 SE 或可信执行环境 TEE 组件从硬件层加密存储、安全启动与防篡改，保障数据安全性、保密性。自毁机制能迅速销毁数据，防止泄露，全方位保护用户数据权益。

3.3.3. 《加州消费者隐私法》(CCPA)

《加州消费者隐私法》（CCPA）是美国加利福尼亚州为增强该州居民隐私权利和消费者保护而制定的州法规。作为美国首部关于数据隐私的全面立法，CCPA 旨在赋予加州居民对自身个人信息更强的控制权，为消费者隐私和数据安全保护构筑起坚实的法律屏障。

在数据隐私保护趋势下，PlugOS 严格遵循《加州消费者隐私法》（CCPA）要求。设计上，杜绝数据采集与行为分析，无广告、无推荐、不监听、不上传，充分尊重消费者对个人信息的控制权，契合 CCPA 赋予消费者主导权的核心精神。功能实现中，TEE 和 SE 起关键作用，符合 CCPA 对信息保密性的要求；数据保护采用高强度加密算法与密钥管理机制保障保密性，用哈希算法校验完整性，满足 CCPA 对信息质量的要求。此外，其支持暴力破解清除、胁迫密码自毁等机制，高风险场景下可主动销毁信息，切实保护消费者信息权益，全方位践行 CCPA 要求。

3.4. 标准制定与行业贡献

我们以推动信息安全行业标准完善为己任，深度参与编制了多项关键安全标准规范。其中包括：

- **行业标准：**《基于可信执行环境（TEE）的 eSIM 技术要求》（YD/T 6153-2024）。
- **团体标准：**《金融安全芯片中央处理器安全技术规范》（T/BFIA 007—2021）、《移动智能终端数字车钥匙信息安全技术要求》（T/TAF 074—2020）。

通过深度参与标准制定，我们不仅为行业贡献了我们的技术洞察，更将这些高安全要求前置融入 PlugOS 的技术架构设计，使我们的产品从研发源头就锚定了行业顶尖的安全基准。

3.5. 独立的第三方安全审计与内部合规管理

PlugOS 建立了“外部独立验证 + 内部持续改进”的双轨合规机制：

- **外部独立验证**：我们定期聘请业界顶级的、独立的第三方安全机构，对 PlugOS 操作系统、硬件设计、加密实现及宿主机客户端 App 进行全面的渗透测试和源代码级别的安全审计。
- **内部合规闭环**：我们设立了专业合规管理团队，动态追踪全球法规与标准变化，每半年至少进行一次全流程合规内审，确保管理、研发、交付环环相扣，持续强化 PlugOS 的合规有效性。

4. 安全威胁模型与设计原则

一个健全的安全系统始于对威胁的深刻理解和清晰的设计哲学。安全威胁模型是 PlugOS 安全设计的基础，通过界定 “保护什么”“防御谁”“划分信任边界”“无法解决什么”，清晰划定安全防护的核心范围。

4.1. 核心保护资产

PlugOS 被设计用于保护存储或运行在 PlugOS 内部的数据与应用，这些资产包括但不限于：

- **密钥与凭据：**加密密钥、身份认证令牌、各类账户密码等。
- **用户隐私数据：**文件、消息记录、通讯录、日历、照片、音视频等。

- **通讯元数据与内容**：通信行为本身、会话内容、关系图谱等。
- **金融资产与身份凭证**：数字货币私钥、网上银行凭证、数字身份证明等。
- **位置与行为轨迹**： 地理位置信息、应用使用记录、网络访问历史等。

4.2. 核心防御对象（攻击者模型）

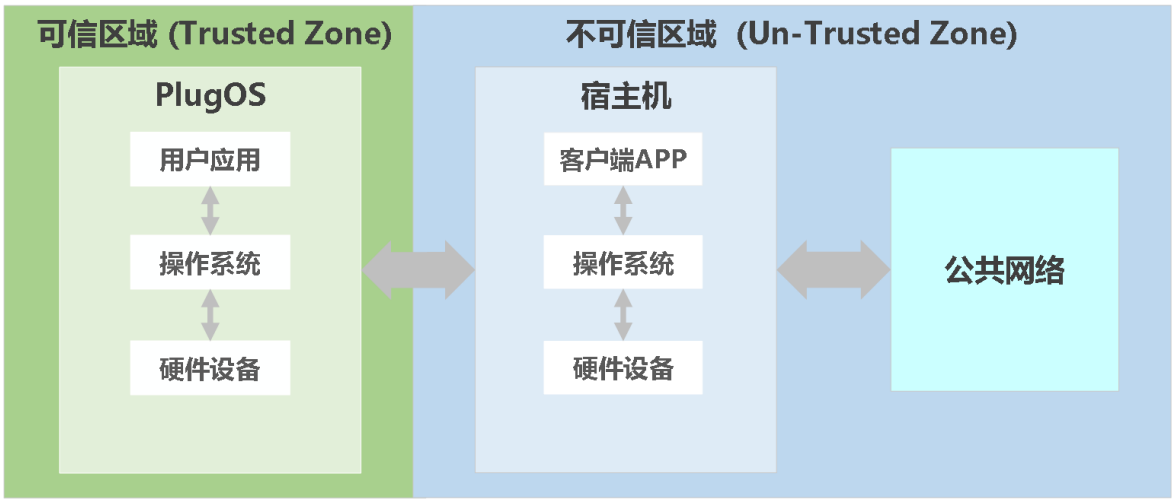
PlugOS 的防御模型覆盖了多维度、多层次的攻击者类型，包括但不限于如下几种常见类型：

- **物理胁迫者**：在人身胁迫或物理压力等场景下，试图强迫用户解锁设备、交出凭据的个体。例如外出时遭遇劫持，用户直接反抗可能危及生命，而顺从意味着财务和隐私被攻击者双重洗劫。
- **物理攻击者**：在设备丢失或被盗后，试图通过冷启动攻击 (Cold Boot Attack)、JTAG 调试、芯片拆焊读取 (Chip-off Forensics) 等物理手段提取设备内数据的技术人员。设备被盗后，攻击者通过冷启动、芯片拆焊等手段尝试提取 PlugOS 内部数据。
- **供应链攻击者**：在设备的生产、运输、分发或软件更新环节中，试图植入硬件后门、恶意固件或被污染软件包的内部或外部人员。
- **宿主机入侵者**：已完全控制 PlugOS 所连接的宿主机（PC 或手机）的攻击者，试图通过宿主机侧的恶意软件对 PlugOS 进行攻击。
- **恶意应用提供者**：诱导用户在 PlugOS 内部安装恶意应用，试图窃取其他应用数据、进行未授权操作或建立隐蔽信道的攻击者。
- **网络攻击者**：通过中间人攻击 (MITM)、DNS 劫持、恶意 Wi-Fi 热点等方式，试图窃听或篡改 PlugOS 网络通信的攻击者。

4.3. 信任边界（零信任）

PlugOS 的核心安全理念是“零信任”，即默认不信任任何网络、外部应用及相邻系统。信任边界被显式地、最小化地划分，以降低系统的攻击面。

- **可信区域 (Trusted Zone)**： PlugOS 硬件设备及其固件、经过签名验证的 PlugOS 操作系统。所有用户数据和应用运行于此区域内。
- **不可信区域 (Untrusted Zone)**：宿主机操作系统、宿主机客户端 App、所有外部网络等。



信任边界区域图

可信区域与不可信区域之间存在一条清晰的、由硬件强制实施的安全边界。两者仅通过一个端到端加密的 I/O 通道进行有限交互。下表清晰地界定了二者的责任与权限：

维度	可信区域（PlugOS）	不可信区域（宿主机）
运行环境	独立硬件 + 可信执行环境 (TEE/SE) + 安全操作系统	宿主机开放系统（如 Android/ iOS/ Windows）
权限范围	管控所有内部应用与数据，拥有硬件级加密与隔离能力	仅作为 I/O 代理，无权限访问 PlugOS 内部任何明文数据
数据存储	硬件加密存储用户数据，数据在内部闭环流通	仅存非敏感配置，无用户数据留存
安全责任	承担用户数据从存储、计算到销毁的全链路安全与隐私保护	仅确保自身代码的完整性及通道安全，不参与核心安全决策

4.4. 无法解决的安全威胁

为保持透明性，我们必须明确指出 PlugOS 威胁模型无法直接覆盖的安全风险。这些风险主要源于可信区域之外的因素，其缓解措施依赖于用户的安全意识和行为。主要为如下两大类：

4.4.1. 用户行为失误带来的风险

PlugOS 旨在防止未经授权的访问，但无法阻止用户主动或被误导后执行的不安全操作，这包括：

- **社会工程学与钓鱼攻击**： 用户被诱导点击恶意链接、下载恶意附件或在仿冒网站中主动输入凭据。
- **凭据泄露**： 用户主动将解锁密码、产品密钥等高权限凭据告知他人，或将其记录在不安全的位置导致泄露。
- **恶意应用授权**： 用户在 PlugOS 内部主动安装来源不明的应用，并授予其过高的权限。

缓解措施：PlugOS 通过权限最小化、应用隔离、网络防火墙等机制提供技术防护，但最终防线仍是用户的安全意识。我们强烈建议用户仅从可信来源安装应用，并审慎授予权限。详见第 11 章《用户可操作的安全核验清单》。

4.4.2. 不可信环境下带来的风险 (宿主机与物理环境)

PlugOS 的安全边界止于其物理硬件。当外部物理环境或所连接的宿主机环境完全被攻击者控制时，可能存在信息泄露的风险。

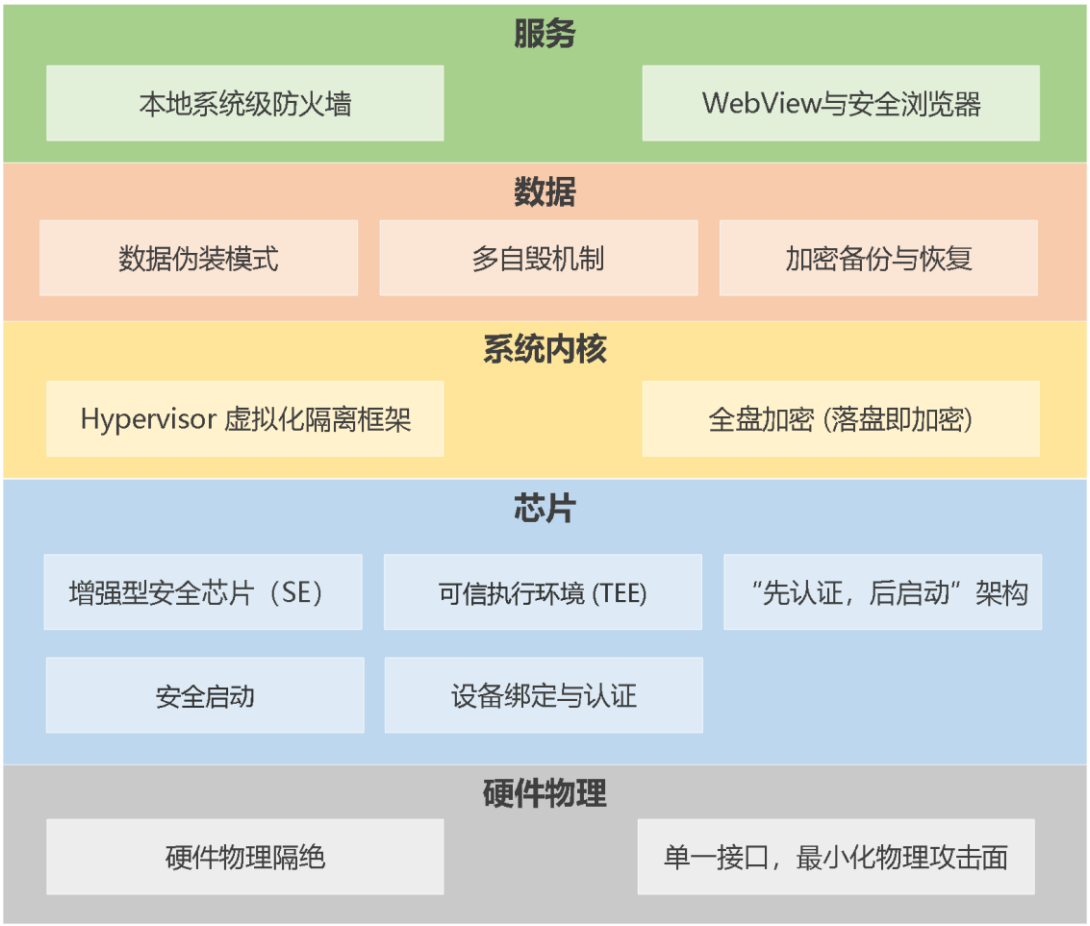
- **物理环境监听**： 攻击者可通过外部隐藏摄像头、窥视等手段，在用户输入密码或查看屏幕时窃取信息。这超出了任何端点设备自身的防护能力。建议用户在操作敏感信息时，确保物理环境的安全。
- **完全失陷的宿主机**： PlugOS 的设计确保了即使宿主机被恶意软件感染，也无法直接访问其内部的静态数据 (Data-at-Rest) 和运行时数据 (Data-in-Use)。但是，数据在显示时 (Data-in-Display) 和输入时 (Data-in-Input) 必须通过不可信的宿主机进行 I/O 代理。因此，一个被内核级恶意软件（如高级键盘记录器、底层截图工具）完全控制的宿主机，理论上可以记录用户的键盘输入和屏幕显示内容。

缓解措施：这是一个在安全、便携和成本之间进行权衡的架构性选择。PlugOS 的宿主机客户端 App 内置了运行时环境安全检测能力，可有效对抗大部分应用层的截屏、录屏和注入攻击。然而，面对来自宿主机操作系统内核层面的攻击，任何应用层防护都无法提供绝对保证。因此，我们建议用户将 PlugOS 连接到自身拥有控制权且安全状况良好的宿主设备上，以将此风险降至最低。

5. 安全架构

PlugOS 的安全架构遵循纵深防御的核心思想，以不可篡改的硬件信任根为基石，通过层层递进、环环相扣的安全机制，构建了一个从芯片到应用的全链路可信计算环境。我们不仅沿用并强化了 AOSP (Android Open Source Project) 成熟的安全模型，更通过架构性的创新，旨在抵御从物理入侵、供应链攻击到强制胁迫等极端威胁，确保用户数据的机密性与完整性。

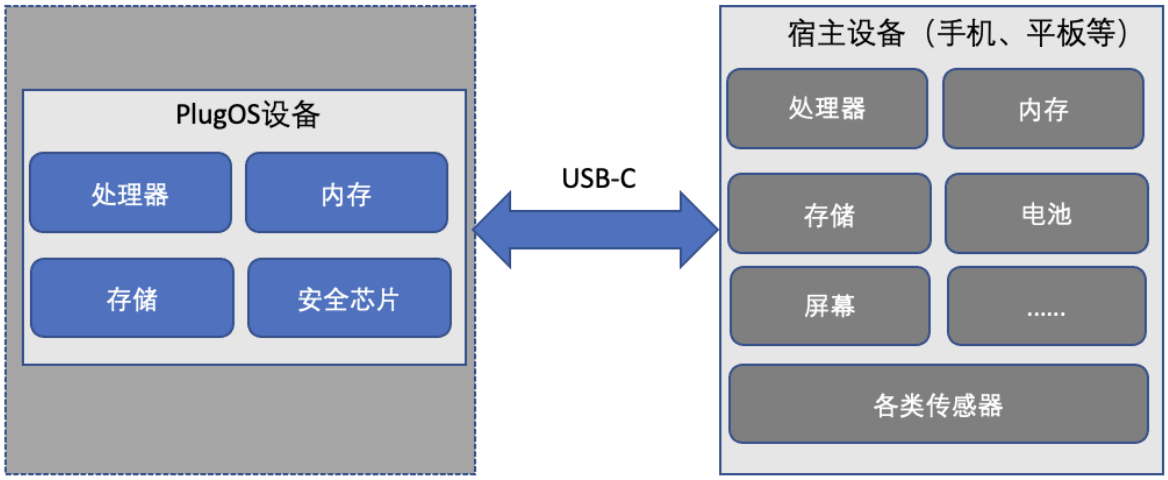
本部分将从硬件物理、芯片、系统内核、数据及核心服务，逐一解析 PlugOS 的核心安全机制。这些机制的设计目标是提供基于架构、可验证的安全，而非基于承诺的信任。



PlugOS 的安全架构图

5.1. 硬件物理隔绝与攻击面最小化

这是抵御外部威胁的第一道防线，也是最直观的一道防线。



硬件组件架构图

硬件物理隔绝：PlugOS 作为一个功能完备的独立计算和存储单元，拥有独立的高性能处理器、高速内存和大容量存储，与宿主系统（用户的电脑或手机）在物理上完全隔离。这意味着宿主机操作系统（用户的电脑或手机等）在架构上无法访问 PlugOS 的内存地址空间或存储芯片。即使宿主机被恶意软件完全控制，也无法跨越这条物理边界。

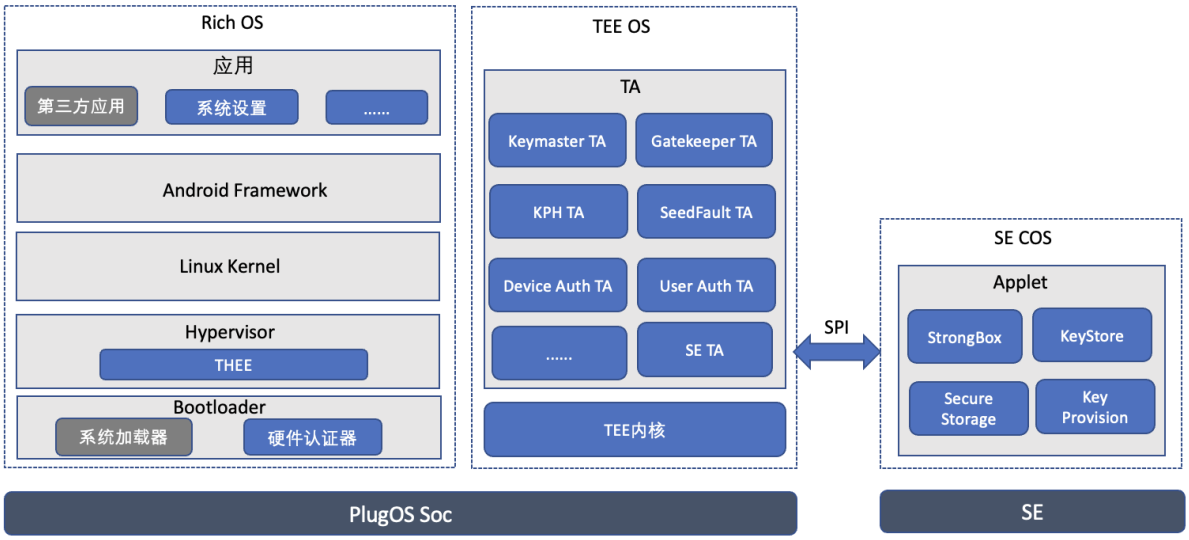
最小化物理攻击面：PlugOS 的硬件设计遵循极简原则。设备不包含蜂窝基带、NFC、GPS 等复杂的射频组件或不必要的传感器，仅通过一个经过强加密协议保护的 USB-C 接口与外界交互。这种设计极大地收敛了物理和软件的攻击面，从源头上降低了被远程或近场攻击的风险。

5.2. 芯片级安全隔离

硬件是所有安全的起点。PlugOS 的安全模型始于一个由硬件强制保障、无法被软件篡改的信任根。

5.2.1. 芯片级安全隔离底座

PlugOS 的安全隔离底座是基于安全芯片 SE 和可信执行环境 TEE，确保关键操作不可篡改。



PlugOS 芯片隔离架构

增强型安全芯片 (SE)：部分型号的 PlugOS 设备内置了获得 CC EAL6+ 认证的独立安全芯片 SE。SE 是一个具备防物理篡改能力的微型安全计算机，为加密密钥等核心机密信息提供了物理保险箱级别的保护；CC EAL6+是目前最高等级的芯片安全认证之一。PlugOS 深度整合了安全芯片能力并原生支持 Android StrongBox Keymaster 规范，确保密钥的生成、存储和使用全程在硬件内部完成，无法被包括操作系统在内的任何外部软件访问，为加密操作和凭证管理提供了等同于银行卡芯片级别的硬件安全保障。

TEE 可信执行环境：所有 PlugOS 设备均搭载了基于 ARM TrustZone 技术的 TEE，其 TEE OS 核心由业界领先的 TrustKernel 提供，通过了 CC EAL4+ 安全认证并历经十亿级设备量产考验。TEE 为 PlugOS 的用户与设备双重身份认证、数据加解密、密钥管理、SE 管理等核心安全操作创建了一个与主操作系统并行的、硬件隔离的运行环境，有效防止了主操作系统漏洞对核心安全功能的影响。

5.2.2. 架构性创新：“认证前置”启动流程

PlugOS 颠覆了传统的“启动后认证”模式。传统的安全启动（Secure Boot）虽然能验证系统签名的完整性，但无法阻止被植入后门的固件在用户认证前执行。例如，当前很多商业化破解软件可以在不经过用户授权的情况下从物理层破解与提取设备上的用户数据，主要是利用设备底层固件的漏洞。PlugOS 从架构上解决了这一问题：在任何系统代码被加载、校验和执行之前，设备必须在芯片级完成用户身份与宿主设备身份的双重认证。**此举杜绝了传统通过物理攻击、供应链污染或底层固件漏洞绕过认证防线的可能性。**例如，即便芯片固件或 Linux 内核

层存在后门，只要未通过硬件安全芯片完成用户和设备双重身份认证，存在后门的供应链固件永远没有机会通电并启动执行。

安全启动：设备启动的每一阶段都经过数字签名验证，形成一条完整的“信任链”。任何未经授权的固件或被篡改的系统镜像，没有被加载和执行的机会，因为它们依赖的磁盘解密密钥在认证成功前不存在于内存中。

设备绑定与认证：PlugOS 只允许连接经过认证授权的宿主设备。首次在宿主机上使用时，用户需要通过 PlugOS 设备的产品密钥进行宿主机绑定。后续连接时，只有经过绑定并通过验证的宿主机才能被识别。宿主机认证是基于宿主机的硬件物理特征进行识别，在首次绑定后 PlugOS 会为宿主机生成绑定密钥对作为后续连接的认证因子。后续只有经过身份验证的宿主机才能与之通信，防止了中间人攻击和非法接入。

5.3. 系统与内核层安全强化

在硬件保障的基础上，PlugOS 通过先进的虚拟化技术和强制性加密机制，构建了强大的软件隔离防线。

基于轻量级 Hypervisor 的内核隔离：传统宏内核架构下，一旦攻击者获得 Root 权限，整个系统便完全失陷。PlugOS 内置了自研的轻量级 Hypervisor (虚拟机监视器)，将操作系统内核的关键组件（如内存管理组件、安全策略管理组件）进行了虚拟化隔离，为每个应用创建独立的、受严格策略限制的安全域。这种设计使得即便单个应用或某个系统服务存在漏洞，也难以横向移动，这限制了漏洞对内核或其他应用的影响范围，提升系统的抗渗透能力。

全盘加密 (落盘即加密)：PlugOS 默认启用文件级全盘加密架构。任何写入存储介质的数据，都会在写入瞬间被硬件加密引擎自动加密。每个文件都使用独立的密钥进行加密，而这些文件密钥又被一个主密钥所保护。这个主密钥由 TEE/SE 安全地保管，并与用户的解锁凭据强绑定。这意味着，即使攻击者通过物理手段（如芯片拆焊）获取了闪存芯片，也无法读取任何有价值的明文信息。

5.4. 数据自毁与安全恢复

除了坚实的传统安全架构，PlugOS 还创新地引入了针对物理胁迫和暴力破解等极端场景的数据防护机制。这是用户数据安全的最后一道防线，确保用户对自己的数据拥有绝对的控制权。

为应对极端胁迫或物理破解情况，PlugOS 内置了多种数据自毁机制。该机制可由连续密码输入错误或用户在解锁界面中主动输入预设的胁迫密码来触发。一旦触发，系统将不可逆地销毁加密密钥，使全盘数据不可逆地销毁。同时，PlugOS 提供了端到端加密的备份与恢复方案，用户可定期将数据安全备份至自己选择的可信存储中，加密密钥由用户自主掌握，实现了自主存储、自主恢复，确保数据主权始终掌握在自己手中。

5.4.1. 胁迫密码

- **工作原理**：用户可以预设一个胁迫密码。当使用此密码解锁时，PlugOS 会无缝删除内部所有数据。
- **应用场景**：在被强制要求解锁设备时，用户可通过输入胁迫密码来保护自身安全和真实数据，为攻击者呈现一个无价值的目标。

5.4.2. 自毁机制

- **触发条件**：
  - 防暴力破解：连续输入错误密码达到用户设定的阈值。
  - 物理防拆（仅部分型号支持）：检测到设备外壳被异常打开或关键芯片受到物理攻击。
  - 胁迫密码触发：用户可将某个胁迫密码配置为触发无声自毁。
- **执行流程**：一旦触发，TEE 或 SE 将执行一个不可逆的加密密钥销毁程序，使全盘加密的数据瞬间变为无法恢复的乱码，从而达到彻底清除所有敏感数据的目的。

5.4.3. 加密备份与恢复

PlugOS 提供的端对端加密备份与恢复能力，确保你的所有数据在备份、传输和恢复过程中始终处于加密状态，最大限度防止未授权访问。备份数据在设备端使用仅用户知晓的密钥进行端到端加密，然后才能导出至用户自选的存储位置（如个人电脑、外部存储设备等）。恢复过程同样需要用户提供密钥在本地完成解密。我们作为服务提供商，全程无法访问用户备份的任何明文内容，确保了用户数据主权在备份和恢复过程中的完整性。

5.5. 关键服务安全增强

PlugOS 对多个与隐私和安全息息相关的核心系统服务进行了深度重构和强化。例如：

本地系统级防火墙：防火墙作为 PlugOS 的核心网络安全组件之一，与系统网络堆栈深度集成，使其具备对所有应用（包括系统应用）网络行为的强制访问控制能力。它在本地运行，不分享或上传任何日志，并能识别和拦截应用内置的追踪器 (Tracker) 和遥测 (Telemetry) 连接。用户可以基于应用、域名、IP 地址、端口等维度，制定精细化的网络访问策略，真正做到一切连接皆可控。

WebView 与安全浏览器：PlugOS 内置的浏览器和应用内 WebView 组件基于 Chromium，并集成了多个领先安全项目的强化补丁集。我们移除了所有 Google 服务依赖和遥测代码，默认禁用高风险的 Web API，开启严格的 Cookie 隔离和追踪保护策略，并强化了 JIT 编译器以抵御内存攻击。这为用户提供了一个不采集、不追踪、不打扰的纯净浏览环境。

6. 隐私架构

与主流操作系统对用户数据和行为默认收集、可选退出的模式相反，PlugOS 严格践行“**设计即隐私 (Privacy by Design)**”的核心原则。我们从不构建更安全的广告平台，而是从架构层面根除任何形式的非必要数据收集。PlugOS 的所有机制都围绕“**数据本地化、行为不被分析、用户完全掌控**”三大目标展开，确保用户的每一项数字操作都只服务于用户自身的意图。

本部分将详细阐述 PlugOS 为实现这些目标所构建的核心隐私技术。

6.1. 零数据收集

在传统移动操作系统中，即使用户关闭了大部分数据共享选项，仍会存在系统级别的后台遥测和行为分析。这些不可见的收集往往用于优化服务或精准广告，但本质上削弱了用户的隐私主权。

零遥测与数据本地化是 PlugOS 隐私承诺的基石：**我们不收集你的数据，因为我们的系统在设计上就没有这个功能。**

- **默认关闭的遥测与分析：** PlugOS 基于 AOSP 构建，但在编译和定制过程中，我们从系统底层、框架层到核心应用层，默认系统性地移除或禁用了所有 Google 服务框架以及 AOSP 内置的遥测 (Telemetry)、崩溃报告和用户行为分析等数据收集组件。在 PlugOS 中，不存在任何会将您的应用使用习惯、系统性能数据或个人偏好等信息发送给设备制造商或软件开发商的后台服务。

- **无广告、无推荐：** 由于不存在用户画像和行为分析，PlugOS 系统全局不包含任何广告或个性化推荐内容。用户的数字体验由其自身意志主导，而非由算法驱动。
- **数据本地化与最小化原则**：我们的理念是，不存储的数据是最安全的数据。我们对系统本身及其内置的所有基础应用（如浏览器、输入法、文件管理器）进行了重构设计，严格遵循数据本地化与最小化原则。例如，我们的输入法只在本地设备上处理用户的输入内容，不进行任何形式的云联想或用户词典上传。
- **零知识模式：**即使是系统厂商 TrustKernel 也无法通过 PlugOS 获取用户的任何敏感数据。用户的所有信息均掌握在自己手中，厂商的角色仅限于提供安全工具。

传统 Android/iOS 等系统，即便开启了限制广告追踪，系统仍会通过遥测上传部分匿名化数据；PlugOS 没有限制开关，因为从一开始就不存在数据收集。

6.2. 传感器虚拟化：阻断硬件指纹追踪

现代应用普遍使用设备指纹 (Device Fingerprinting)来识别和跟踪用户。这类指纹通常结合硬件特征（如 IMEI、传感器 ID、基带信息）、网络环境（IP、DNS、时区）、软件状态等数百个参数来创建唯一用户与设备标识符，即使用户更换账户或清空缓存，也难以避免身份被重识别和持续追踪。设备指纹一般不需要特殊权限，用户难以察觉，会持续造成用户隐私信息泄露并被追踪行为轨迹。

PlugOS 通过系统级传感器虚拟化技术，切断设备指纹的生成路径，从而有效保护个人身份和行为隐私。

6.2.1. 身份标识虚拟化

对于那些可被用作唯一标识的硬件 ID，PlugOS 进行了虚拟化处理。对于请求此类信息的应用，系统会有选择地提供通用的、无意义的默认值，或者为不同应用提供不同的随机值，而非真实的硬件序列号、SIM 卡信息 (IMSI/ICCID)、MAC 地址等。

6.2.2. 传感器数据模拟

用户可以通过一个集中的隐私控制面板，按需模拟各类环境信息，从而向应用提供虚假但合理的数据，以满足其运行需要，同时保护真实信息。例如：

- **虚拟地理位置**：用户可设定一个固定的虚拟位置，或一条动态的虚拟移动路径。

- **虚拟网络状态**： 模拟不同的蜂窝网络运营商、网络类型及基站信息。

6.2.3. 硬件直通动态切换

用户在需要时，可以通过权限确认，将宿主机的真实硬件（摄像头、麦克风、蓝牙）直通给 PlugOS 内的特定应用，在功能可用与隐私保护之间灵活切换。用户可以随时撤销授权，确保硬件访问随用随开、用完即关。

这种设计确保即便是最激进的指纹追踪算法，也难以建立可靠的身份关联，从而最大限度地保护用户与设备的匿名性与去标识化。

6.3. 透明可控的网络连接

网络流量是数据泄露的主要渠道。许多应用在未提示用户的情况下，向第三方服务器上传日志、SDK 数据或行为信息。

PlugOS 内置了系统级的防火墙，赋予用户前所未有的网络流量洞察力和控制力，让用户对每一个数据连接做到知情、可控、可溯。其核心工具是第三章提及的内核级防火墙，本节侧重其隐私保护功能。

- **追踪器识别与屏蔽**：内置数据库可检测应用中常见的广告 SDK、分析 SDK，并提醒用户该连接潜在的隐私风险。用户可选择屏蔽这些第三方追踪器。
- **连接审计**：防火墙会实时记录系统中所有应用的网络连接请求，并以清晰、易于理解的方式呈现给用户，包括目标域名、IP、协议，避免暗中上报，让隐藏在应用背后的数据外传行为无所遁形。用户可选择屏蔽某些应用或目标服务器的网络连接。
- **白名单模式**：对于处理高度敏感数据的场景，用户可以启用严格的“白名单”模式，即默认禁止所有网络连接，仅允许其访问用户手动批准的特定域名或 IP 地址。对于完全不需要联网的场景，用户可以一键彻底切断其所有网络权限，杜绝其通过任何方式泄露信息的可能性。

7. 宿主机客户端 App

宿主机客户端 App 是 PlugOS 在手机或电脑上的配套应用，它的主要作用是帮助 PlugOS 调用宿主机的屏幕、键盘等外设，实现交互和显示。本部分将从定位、职责、边界三个方面阐明：该 App 不会成为 PlugOS 的安全风险源。

7.1. 核心定位：一个受限的“I/O 代理”

宿主机客户端 App 的设计严格遵循最小权限和零信任原则。它在 PlugOS 的安全模型中被明确划分在“不可信区域”（参考 4.3 节），其核心定位是一个功能受限的“I/O 代理 (Input/Output Proxy)”，充当用户与 PlugOS 硬件设备之间的一座桥梁。换句话说，即便宿主机客户端 App 出现漏洞、被黑客篡改，甚至被完全控制，也无法获取或解密 PlugOS 内部的数据。

7.2. 职责与限制：它能做什么与不能做什么

为清晰界定其能力边界，下表详细列出了客户端 App 的被允许的职责和被架构限制的行为：

被允许的职责（能做什么）	被架构限制的行为（不能做什么）
1. 转发输入： 接收宿主机的键盘、鼠标、触控等输入信号，原封不动地通过端到端加密通道发送给 PlugOS 硬件。	1. 解密任何数据： 所有加密密钥都安全地存储在 PlugOS 硬件的 TEE/SE 中，从未也不会离开硬件。App 无法获取密钥，因此无法解密它所传输的任何数据。
2. 渲染输出： 接收来自 PlugOS 硬件的屏幕图像帧数据流，在宿主机屏幕上进行渲染显示。	2. 访问明文数据： App 只是作为 PlugOS 与外界沟通的通道，它无法探知网络通信的具体内容。
3. 代理加密网络： 作为一个网络出口，将来自 PlugOS 的加密网络流量转发到互联网。	3. 执行核心逻辑： 用户的身份认证、数据加解密、文件系统读写、应用运行等所有核心计算任务，全部在 PlugOS 硬件内部独立完成。App 不参与任何决策过程。
4. 检查自身更新： 连接官方服务器，检查 App 自身是否有新版本，不涉及任何用户数据的交互。	4. 存储用户数据： App 不会在宿主机上存储任何 PlugOS 内部的用户数据、配置或状态。它的设计是无状态的。

7.3. 安全边界：即使被攻破也无法威胁 PlugOS

客户端 App 不在 PlugOS 的可信边界之内，属于不可信区域，即使宿主机 App 被恶意篡

改，甚至被黑客完全控制，它也无法解密或窃取任何 PlugOS 内部的数据。PlugOS 的安全性来自于“独立硬件 + 系统加密 + 严格边界”，而非依赖客户端 App 的行为。这种设计消除了闭源宿主机 App 带来的信任风险。

8. 安全组织和人员管理

PlugOS 的安全保障不仅来自技术架构，还来自完善的组织与管理体系。 我们设立了专门的安全研发、测试、合规与应急响应团队，形成从研发到运营的全流程安全闭环。

- **安全研发与测试**：持续探索安全前沿技术，结合多维度测试与渗透验证，确保 PlugOS 安全性能不断进化。
- **合规与治理**：紧跟全球法规与行业标准，严格审查数据处理活动，满足 GDPR、PIPL 等法规要求。
- **应急响应**：建立快速响应机制，覆盖安全事件预防、处置与追踪，保障服务稳定。
- **人员管理**：员工从招聘、入职、在岗到离职，均执行严格的背景审查、保密义务、分级权限与安全培训，确保信息安全责任落实到人。

9. 安全开发周期管理

PlugOS 在软件开发全流程中嵌入安全与隐私要求，形成符合国际标准的 SDL 管理体系：

- **需求与设计**：开展安全威胁建模与合规评估，将安全指标前置化，确保架构层面规避风险。
- **安全开发**：遵循国际安全编码规范（NIST、ETSI、OWASP 等），结合自动化工具与人工审核，杜绝常见漏洞。
- **安全测试**：进行多层次测试与第三方合规验证，包括加密强度、数据保护机制及渗透测试，形成专业安全报告。
- **持续保障**：产品发布后，持续推送安全更新，监测漏洞并快速修复，确保 PlugOS 在全生命周期内安全可控。

10. 安全运维

PlugOS 的安全不仅体现在技术架构和机制层面，更体现在持续的运维保障、合规遵循和

外部认证，践行着业界最高的安全标准。我们深知，用户信任的基础不只是自我宣称，而是经得起验证、审计和认证的安全运维管理体系。

10.1. 安全更新与运维

PlugOS 构建了一个安全、透明、可追溯的更新机制：

- **加密签名更新包：**所有更新均由官方签名并通过加密通道分发，更新前必须通过数字签名和完整性验证，防止恶意更新。
- **差分更新机制：**在确保安全性的同时，减少更新包体积，降低更新对用户体验的影响。
- **快速回滚能力：**一旦发现更新存在兼容性或潜在风险，用户可一键回滚至上一个稳定版本。
- **最小权限执行：**更新进程严格最小化权限，避免更新服务本身成为攻击入口。

10.2. 安全应急响应中心

我们相信，与安全社区的开放合作是提升产品安全性的关键。为此，我们建立了标准化的产品安全应急响应中心，为用户提供全生命周期的安全响应：

- **安全技术支持：**针对客户在使用中遇到的安全问题，提供实时响应与解决方案，形成产品安全运维 + 客户安全管理的协同闭环。
- **漏洞奖励计划**： 我们积极鼓励并奖励全球的安全研究人员、学者和白帽子黑客对 PlugOS 进行安全测试。我们设立了漏洞奖励计划，对发现并负责任地向我们报告有效安全漏洞的个人和团队提供现金奖励。
- **公开的漏洞披露政策**： 我们制定并公开了详细的漏洞披露政策，为安全研究社区提供了清晰、安全的漏洞上报渠道。我们承诺在收到报告后，会及时进行确认、评估，并与报告者保持沟通，在修复漏洞后予以公开致谢。
- **跨行业合作**：我们持续与安全厂商、科研机构和开源社区建立协作渠道，及时获取威胁情报并响应。

11. 用户可操作的安全核验清单

为帮助用户最大化地利用 PlugOS 的安全能力，我们建议用户定期检查以下安全核验清

单：

- **保管好产品密钥：**用户需要妥善保管产品密钥。若担心产品密钥泄露，可在 PlugOS 设置中重置产品密钥。
- **检查绑定主机：**定期在设置中审查已绑定的宿主机列表，移除不再使用或不受信任的设备。
- **权限最小化：**遵循随用随开的原则，仅在需要时为应用授予相机、麦克风、定位等敏感权**限。**
- **配置网络白名单：**对于处理高度敏感数据的应用，利用防火墙功能限制其网络访问。
- **启用防暴力破解：**根据风险评估，开启输错密码 N 次后自动自毁的功能，并务必做好数据备份。
- **设置胁迫密码：**为应对潜在的人身胁迫风险，预先设置好伪装模式的密码。
- **定期备份数据：**数据是无价的，定期备份数据，防止数据丢失。
- **保持系统更新：**及时安装官方发布的安全更新，确保系统处于最佳防护状态。

12. 结论

PlugOS 不仅仅是一个产品，更是一种安全理念的实践。它通过将信任根基置于独立的、可验证的硬件之上，结合多层防御架构和前瞻性的隐私保护设计，为用户提供了一个真正意义上的数字保险箱。

PlugOS 凭借其可验证的硬件信任链、独立第三方的安全认证、以及独特的零信任架构和数据自毁机制，为那些对数据主权和个人隐私有极致要求的用户，提供了一个可靠、强大且透明的解决方案。我们相信，通过将控制权完全交还给用户，PlugOS 正在为移动安全的未来树立新的标杆。