Fleet Hub 安全白皮书 v1.0

1. 介绍

Fleet Hub 是一款专为第三方系统集成而设计的打印机集群控制接入设备。在提供标准化 RESTful API 接口的同时，它在系统架构的各个层面嵌入了层次化的安全控制。我们深知，对于将打印能力集成到自身平台的服务商和软件开发者而言，安全不是可选项——而是一项基本的设计要求。

本白皮书全面介绍 Fleet Hub 的安全架构与技术实现，帮助合作伙伴和开发者评估和理解我们的安全措施。如有安全相关的问题或建议，请联系：security@bambulab.com。

2. 硬件安全基础设施

Fleet Hub 的安全架构以基于硬件的信任根为锚点。以下机制为密钥、固件完整性和运行时操作提供抗篡改保护，为整个软件栈建立了基于硬件强制执行的信任根（HRoT）。

图 1：Fleet Hub 硬件外形

- **安全启动：**Fleet Hub 支持基于硬件的安全启动，能够确保启动过程中加载的每一个固件组件都是 Bambu Lab 官方签发的固件，防止未授权或恶意固件在设备上运行
- **可信执行环境（TEE）：**TEE 提供了一个基于硬件隔离的安全执行环境。关键的认证逻辑和密钥运算在 TEE 中运行，与通用操作系统隔离。即使系统层遭到攻击，TEE 内的操作仍受到硬件保护
- **硬件安全引擎：**Fleet Hub 内置专用硬件加解密引擎，支持 AES、RSA、ECDSA、SHA 等主流密码学算法。一方面加速密码学运算，另一方面有效降低密钥材料被软件层攻击提取的风险
- **安全存储（RPMB）：**通过将 RPMB（Replay Protected Memory Block）与 TEE 结合，Fleet Hub 为设备证书和密码哈希等关键资产实现了安全存储。RPMB 是存储设备内的受保护分区，通过签名和防重放机制确保数据只能由 TEE 访问，防止未经授权的读写操作
- **硬件 Key Ladder：**启动和运行过程中使用的固件经过加密。加密密钥通过硬件 Key Ladder 机制保护——这是一种分级密钥推导机制，根密钥永久嵌入硬件中，派生密钥在运算时临时生成。软件层无法在任何环节获取明文密钥
- **eFuse（OTP）：**信任根、固件签名公钥哈希等关键配置信息存储在 eFuse 中——eFuse 是芯片内部一次性可编程的存储区域，写入后由硬件强制保护，任何软件手段均无法篡改
- **调试口永久关闭：**JTAG、SWD 等硬件调试接口出厂时通过 eFuse 永久关闭，且无法重新开启

以上机制构成一条相互依赖的信任链：eFuse 存储安全启动所需的硬件强制验证密钥哈希；安全启动在执行前验证固件完整性；Key Ladder 在不向软件暴露密钥的前提下完成固件解密；TEE 将运行时密钥与可能遭到入侵的通用操作系统隔离；RPMB 通过 TEE 中介访问保护持久化凭据。这些控制措施的组合，显著提高了对平台发起攻击所需的成本、复杂度和技术门槛。

3. 系统安全

Fleet Hub 的系统安全架构通过分层纵深防御机制，将硬件信任根延伸至软件栈。在默认安全策略和强制权限隔离下运行，其设计目标不仅是防止初始入侵，更要在单个组件被利用后限制影响范围，使跨安全边界的横向移动极为困难。

- **Verified Boot 与文件系统加密：**Secure Boot 保障启动链中固件的完整性，

Verified Boot 则在此基础上向上延伸——在系统启动时验证文件系统分区的完整性，确保操作系统运行环境本身未被篡改。二者共同构成从固件到运行操作系统的完整性验证链。Fleet Hub 还对关键系统分区启用了文件系统加密，即使攻击者通过物理手段直接读取存储芯片（"dump flash"），得到的也只是加密后的内容，无法还原为可用的固件或系统数据。

- **强制访问控制（MAC）：**Fleet Hub 在操作系统层启用强制访问控制机制。与传统自主访问控制不同，MAC 由系统统一定义和强制执行安全策略——每个应用只能访问被明确授权的系统资源，无法自行提升权限或访问其他组件的数据。即使某个组件遭到利用，攻击者的操作空间也被严格限制在该组件的权限边界内，有效防止单点突破演变为全面控制。

- **内核安全加固：**KASLR（内核地址空间布局随机化）使内核加载时的内存基地址每次随机化，令攻击者无法预先确定内核关键函数的位置，大幅增加代码重用类攻击（如 ROP 攻击）的难度。同时，Fleet Hub 对/dev/mem 等高危内核接口进行了限制，降低了攻击者通过这些接口直接读写物理内存的可能性

- **固件加密与离线安全升级：**发布的固件经过加密和签名双重处理。固件加密增加了逆向分析的难度，使攻击者难以从固件中提取信息或寻找可利用的漏洞。固件签名确保升级包的完整性和来源可信——设备在执行升级前验证签名，验签失败则拒绝安装，防止被篡改或伪造的固件通过升级通道进入设备

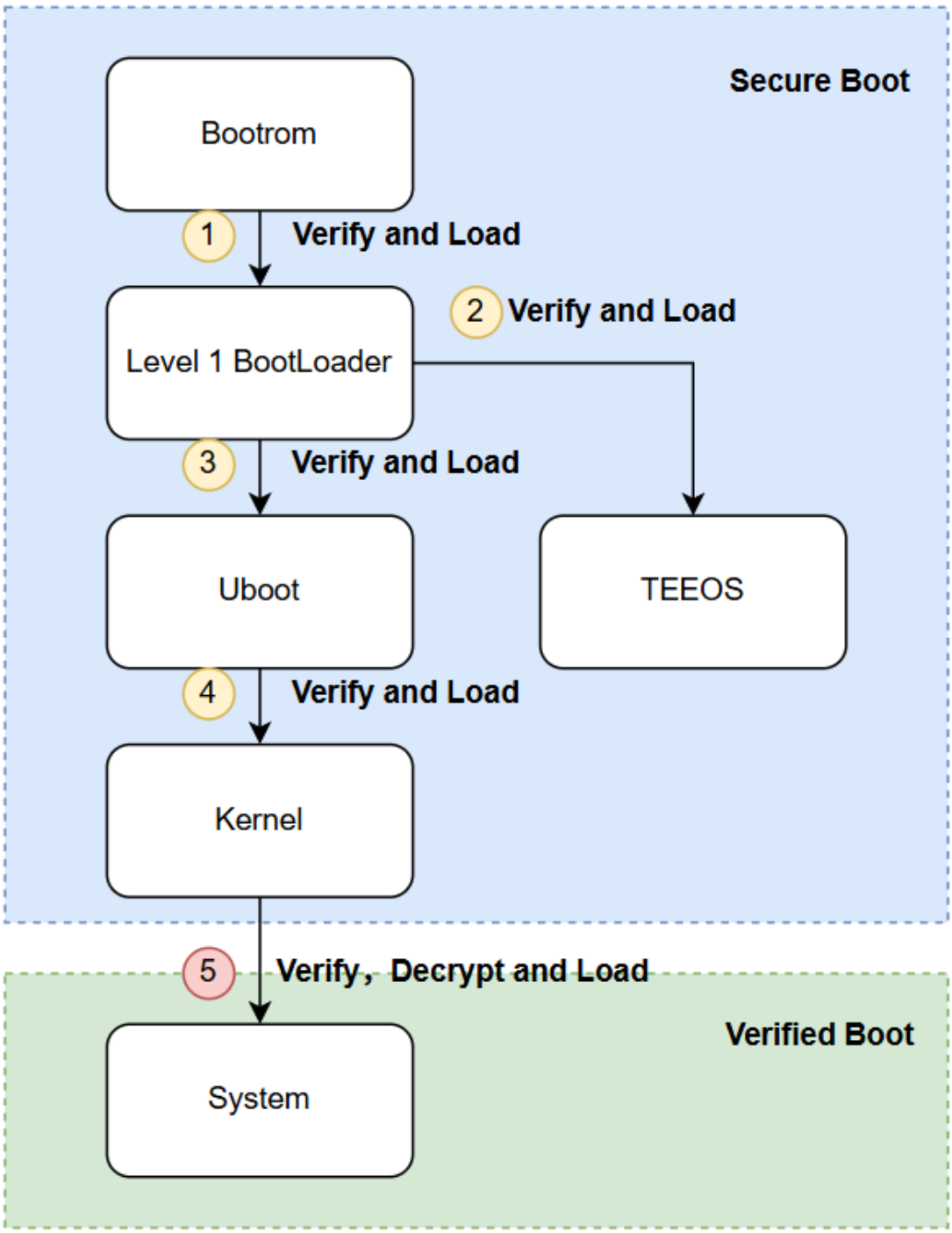

图 2：安全启动 + 验证启动 + 文件系统加密

除以上默认保护外，Fleet Hub 在设备使用生命周期中还提供两项用户可触发的安全功能。日志导出默认加密；恢复出厂设置可根据用户需要执行：

- **日志导出加密：**日志导出是故障排查和技术支持的重要工具。导出日志时默认使用 AES-256-CBC 加密来保护机密性。日志导出始终由用户主动触发——Bambu Lab

不会主动采集或拉取设备日志。用户通过技术支持工单提交给 Bambu Lab 的诊断日志，在工单结束后 14 天自动删除

- **恢复出厂设置：**当 Fleet Hub 报废、转交或需要重新部署时，恢复出厂设置将彻底清除设备上的所有用户数据——包括激活信息、账号凭据、系统日志、模型文件缓存和所有临时数据。设备自动重启至未激活初始状态，确保退役后不残留任何数据

4. 网络与通信安全

硬件信任根与系统层加固的组合，显著提高了针对物理攻击向量的防护门槛。而网络服务和通信是 Fleet Hub 的核心功能——也是其最主要的远程攻击面。

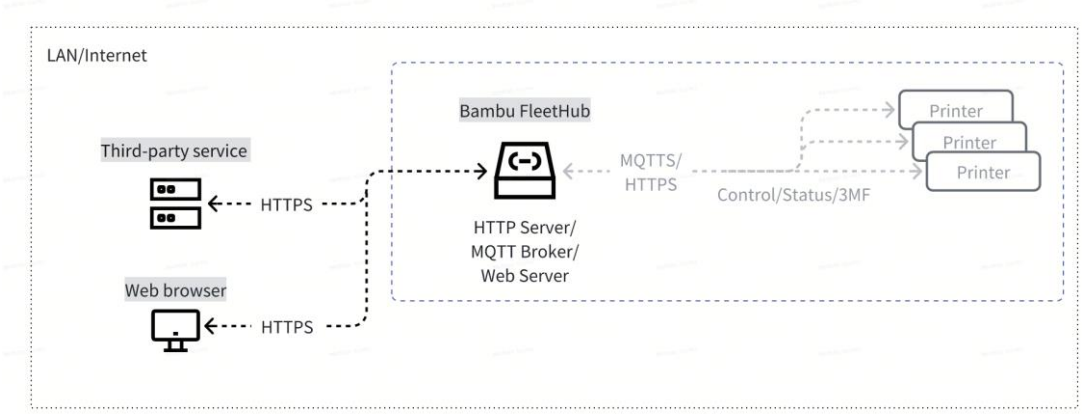

图 3：通信拓扑图

Fleet Hub 在架构设计阶段即将网络与通信安全作为一等优先事项。作为部署在客户可控网络中的企业设备，我们对企业网络兼容性和出站流量控制给予了特别关注。关键措施如下：

- **攻击面缩减：**仅开放运行必需的端口，所有其他端口默认关闭，使攻击者可利用的切入点降至最低
- **全链路 TLS/mTLS：**除 SSDP 服务外，其他链路均采用 TLS/mTLS
- **企业网络接入支持：**Fleet Hub 支持 WPA2-Enterprise 协议，覆盖 EAP-TLS，PEAP(MSCHAPv2)和 TTLS(MSCHAPv2/MSCHAP)
- **数据不出局域网：**Fleet Hub 完成激活后，不主动向外部网络发起任何数据上传或控制连接。所有用户数据和打印操作均保留在局域网内。

Fleet Hub 完成激活后，仅开放以下几类通信端口，所有端口开放情况如下表所示。所有其他端口默认关闭。除 SSDP 服务仅用于局域网内广播设备存在外，其他链路全部使用了 TLS/mTLS。

端口	协议	加密方式	用途
TCP/443	HTTPS	TLS	Web 运维管理界面，仅在设置 web 账号后开启
TCP/8888	HTTPS	mTLS（双向）	第三方服务 API / 模型文件传输
TCP/1883	MQTTs	mTLS（双向）	Fleet Hub 与打印机控制通道
UDP/1990、1991、2021、2022	SSDP	无加密	局域网设备发现

表 1：Fleet Hub 端口开放情况

5. 身份认证与访问控制

Fleet Hub 在身份与访问控制层采用 证书身份 + 账号权限 + 访问令牌 的组合机制。证书用于建立设备与服务之间的机器身份信任，账号用于界定可执行操作，令牌用于控制会话有效期与调用边界。三者共同构成 Fleet Hub 的访问控制基线。

5.1 证书体系

Fleet Hub 的通信端点采用 X.509 终端证书体系，覆盖三类实体：Fleet Hub 设备、3D 打印机设备、第三方服务。Fleet Hub 与打印机证书在产线注入，单设备唯一；第三方服务需向 Bambu Lab 注册后获取接入证书。证书是 mTLS 的信任基础，除 Web 运维管理页面外，其余核心链路均通过 mTLS 建立双向认证（最低支持 TLS 1.2），从连接建立阶段即阻断未授权端点接入。

Fleet Hub 激活 & 证书绑定

Fleet Hub 使用前需要先激活，设备激活过程主要用于建立并固化三方信任关系：

Fleet Hub 先验证第三方服务证书并生成 Active Ticket；第三方服务将 Ticket 提交云端换取签名 Active License；Fleet Hub 验签通过后完成激活。完成激活后，设备身份、服务身份与授权关系进入可验证状态，为后续 API 调用和设备控制提供信任前提。完成激活后，Fleet Hub 也跟三方服务证书建立了绑定关系，其他服务的证书，即使是由 Bambu Lab 合法签发的，也会被该 Fleet Hub 拒绝。

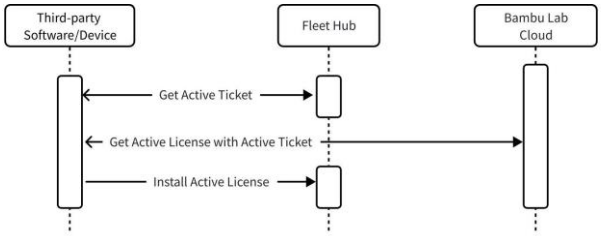

图 4：设备激活过程

5.2 账号体系

如果说证书体系负责“机器是谁”，那么账号体系则负责“谁可以做什么”。Fleet Hub 将机器身份认证与操作权限认证分层设计，避免仅依赖单一凭据模型造成权限扩散风险。Fleet Hub 中主要有 **Local API** 和 **Web 运维管理后台**需要使用账号体系。

Local API 账号

Local API 账号在激活阶段创建，是后续程序化接口调用的必选凭据。系统仅支持一个 Local API 账号。密码强度要求为：不少于 8 位，且必须包含数字、大写字母、小写字母和特殊字符。账号及密钥仅存储在 Fleet Hub 内部安全存储区域，不提供明文导出能力。使用 API Account 登录后，系统签发 JWT Token 用于后续请求，令牌过期后需重新认证，以降低会话被长期滥用的风险。注意，如果 Local API 账号密码丢失，将无法找回，只能恢复出厂设置，请妥善保管 Local API 账号和密码。

重要提示：如果密码丢失，唯一的恢复方式是恢复出厂设置，该操作将清除所有激活信息和数据。请妥善保管凭据。

Web 运维管理后台账号

Web Client Account（Web 运维管理后台账号） 默认不存在，属于可选运维账号；仅可通过已认证的 API Account 进行创建。系统仅支持一个 Web Client Account。Web 界面采用用户名+密码登录，通信通道为 TLS 单向加密。创建时系统会进行弱密码检查，拒绝常见弱密码。若不创建 Web Client Account，则无法登录内置 Web 运维界面，可减少该入口的暴露面与攻击面。

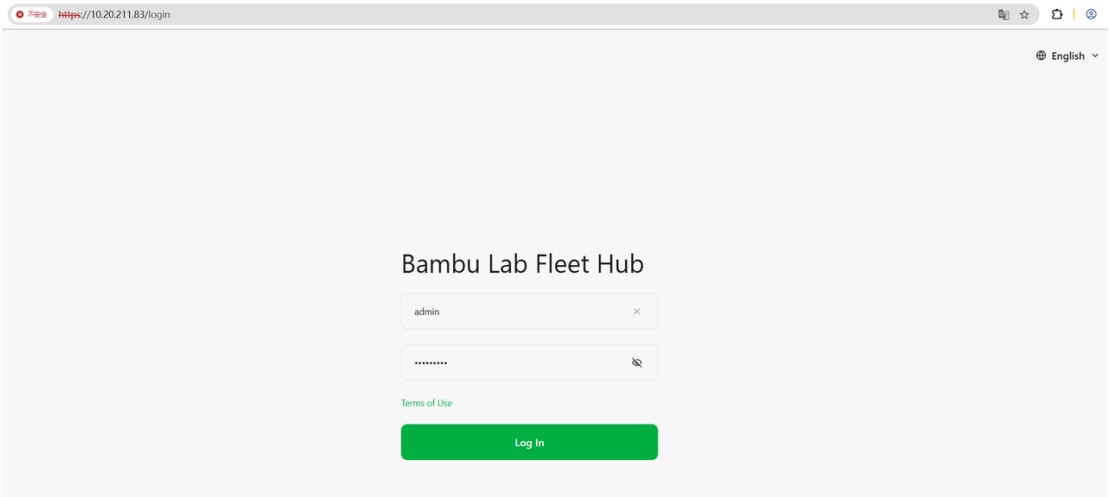

图 5：Web Client 管理后台

密码安全建议：使用高强度、不可复用的独立密码；建议长度不少于 12 位；避免与 API 账号共用密码；在人员变更或疑似泄露后立即轮换，并通过企业级凭据管理工具统一保管。

6. 模型与数据保护

如果说身份认证和访问控制解决的是"谁可以访问、如何建立信任"的问题，那么本章解决的就是"数据在存储和传输过程中是否安全"的问题。Fleet Hub 在打印任务执行过程中会接触服务商最核心的业务资产——客户委托的模型文件，以及打印过程中产生的状态数据和日志。Fleet Hub 在模型传输、本地存储和数据生命周期管理上均采取了针对性的保护措施。

- **模型加密上传：**第三方服务向 Fleet Hub 上传模型文件时，传输通道基于 mTLS 加密的 HTTPS（TCP/8888），确保文件在传输过程中不被截获或篡改
- **模型加密下载：**打印机从 Fleet Hub 下载模型时使用 HTTPS 加密传输。若打印机需从第三方存储服务器直接下载（自定义 URL 下载场景），同样强制要求使用 HTTPS，不支持明文 HTTP。若第三方存储使用自签名证书，需通过 Fleet Hub API 预先将根 CA 或中间证书链（PEM 格式）注入打印机，完成信任链配置后方可使用
- **数据不出局域网：**激活后，Fleet Hub 不向外部上传任何数据。模型文件存储在本地，不会传输至 Bambu Lab 云端或任何其他外部服务
- 本地数据存储：Fleet Hub 提供 40GB 本地存储，存储空间不足时自动删除旧文件。

- **模型加密存储（规划中）**：当前版本模型文件以明文形式存储于 Fleet Hub 本地。后续版本计划支持模型文件的静态加密存储，防止攻击者通过物理接触设备获取明文模型数据。在此之前，建议将 Fleet Hub 部署在物理访问受控的环境中

除模型文件外，Fleet Hub 在打印过程中会缓存打印机摄像头的快照，用于第三方服务监控打印状态。快照数据仅存储在 Fleet Hub 本地，同样不会上传至外部网络。用户可以通过恢复出厂设置彻底清除快照缓存。

以下是 Fleet Hub 中各类数据的存储和清理策略：

数据类型	存储位置	保留策略	出厂重置后
激活信息与账号密码	Fleet Hub 本地	设备在役时有效	清除
模型文件缓存	Fleet Hub 本地	存储空间不足时自动删除旧文件	清除
打印机摄像头快照	Fleet Hub 本地	仅缓存最近一次打印任务的最新快照，之前的快照会被覆盖	清除
系统日志	Fleet Hub 本地	用户主动导出，未导出不离开设备	清除
提交至 Bambu Lab 的诊断日志	Bambu Lab 售后系统	工单结束后 14 天自动删除	--

表 2：数据生命周期

7. 安全合规与组织治理

技术措施是安全体系的基础，但安全不是一次性的工程——它需要持续的验证、流程的保障和外部的审计。本章介绍 Bambu Lab 为 Fleet Hub 在组织层面建立的安全合规机制。

安全认证：Bambu Lab 已获得以下国际安全与隐私认证，覆盖产品研发、数据处理和运营流程，Fleet Hub 作为 Bambu Lab 产品生态的组成部分，同样受上述认证体系覆盖：

- ISO/IEC 27001：国际信息安全管理体系标准，意味着 Bambu Lab 的研发与运维流程接受第三方年度审计
- ISO/IEC 27701：国际隐私信息管理体系标准，覆盖用户数据的收集、处理与保护规范
- TRUSTe Enterprise Privacy：国际隐私与数据治理框架认证，由专注隐私保护领域的第三方机构评定

安全测试：Bambu Lab 建立了内部安全团队，通过多种手段对产品进行持续的安全验证：

- 内部渗透测试：内部安全团队定期对拓竹产品进行人工渗透测试，模拟真实攻击场景，验证防御措施的实际效果
- 外部渗透测试：Bambu Lab 的产品会周期性邀请独立第三方安全机构进行外部渗透测试和安全评估，以客观视角验证安全体系的完整性
- AI 辅助代码审计：在研发阶段引入 AI 工具对代码进行安全审查，识别潜在的漏洞模式和风险点，在问题进入产品前提前发现
- AI 辅助自动化渗透测试：利用 AI 工具对拓竹产品的网络接口和 API 进行自动化渗透测试，持续检验安全边界的有效性

漏洞赏金与安全反馈：Bambu Lab 欢迎安全研究人员、企业客户和合作伙伴报告 Fleet Hub 相关的安全问题。我们重视每一个安全反馈，并将其纳入产品改进与版本迭代的闭环流程中。

- 漏洞赏金计划：https://bambulab.com/en/bug-bounty-program
- 安全反馈邮箱：security@bambulab.com