Bambu Lab
技术安全白皮书

2025.09

目录

01 介绍

Bambu Lab 深圳拓竹科技有限公司是一家致力于用前沿的机器人技术彻底革新桌面级 3D 打印产业的公司，成立于 2020 年，总部位于中国深圳，在深圳和上海设立了研发中心，并在美国奥斯汀设立了办公室。拓竹科技的产品在诸多关键性能上，实现了数量级上的进步，更是把多色彩打印、支持高性能工程塑料等工业级打印机技术带入消费级产品，让用户在打印过程中能够突破色彩和材料的限制，将创造力提升到了一个全新的水平，找到纯粹的创造乐趣。

虽然初始团队拥有丰富的机器人背景，但是最初在网络安全方面的经验是不足的。社区最先关注到了早期产品中的网络安全问题，并给我们敲响了警钟。这让我们意识到产品的网络安全和用户的隐私数据安全是我们必须做好且责无旁贷的事情。因此，在过去三年里我们把网络安全和用户的隐私数据安全作为公司最重要的事项之一，持续增加相关人员投入，跟业界安全专家、研究机构和行业伙伴的公开合作，并在产品上持续的采取行动来改善我们的产品安全性。

这份安全技术白皮书，记录了拓竹这三年来在网络安全和隐私数据安全领域的不断投入和探索实践。我们深切理解用户对网络安全和隐私数据安全的重视，并将其视为我们运营的基石。我们也衷心感谢社区提出的宝贵意见，正是这些声音鞭策我们不断学习、进步。未来，拓竹科技将继续秉持开放透明，公开合作的态度，以更强大的安全防护能力，为每一位用户的创新之旅保驾护航。

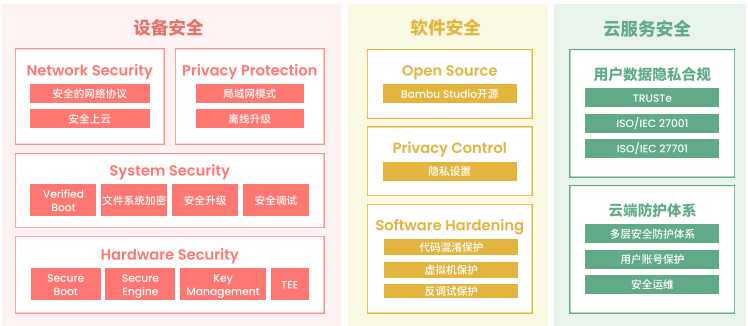

图1：安全防御体系

本白皮书将按下述的结构深入阐述了拓竹 3D 打印机的安全架构、技术原理、功能设计以及相关软件和云服务的隐私保护措施，我们希望本文档能够促进这些措施的架构和实施更加清晰透明。

设备安全：软硬件相结合，构建设备的安全防护，网络安全和数据安全功能
软件安全：通过虚拟机保护和运行时防护手段保护软件，减少用户端软件被攻击的风险
云服务安全：采用云端多层防御机制，通过安全管理和周期性渗透测试保护云端安全性
隐私合规：我们坚信用户的隐私数据是用户的核心价值，我们安全和隐私的组织流程经过国际认证
开源计划：我们从社区学到了很多，也愿意回馈社区。我们尊重开源社区和开源协议，并严格执行开源计划
漏洞赏金计划：寻求与安全专家、研究机构和行业伙伴的公开合作，共同提升我们的安全防护能力

如果您想与我们讨论任何与安全相关的问题，可以联系到我们：security@bambulab.com。我们非常重视每一个用户反馈，并将采取一切必要措施来提升我们产品的安全性。

02 设备安全

在拓竹的产品服务生态中，3D 打印机的产品安全至关重要，而设备安全更是核心环节。一方面，3D 打印机在工作中必然会处理用户的设计模型和参数，未经授权的访问或网络攻击极易导致用户的知识产权和商业机密泄露。另一方面，由于 3D 打印机常在家中使用，一旦被恶意控制，可能引发危险的打印行为，甚至造成火灾等严重安全隐患。

我们坚信，随着 3D 打印市场的日益成熟，用户对设备安全性的要求将持续攀升。卓越的产品安全不仅是未来 3D 打印机的核心竞争力，更是拓竹赢得用户信任、树立行业标杆的关键所在。

2.1 硬件安全

硬件安全基础设施是设备安全的基础，如果没有硬件基础设施的支持，软件层面的安全防护将很容易被破解，密钥也很难被有效保护，用户的网络安全和隐私数据安全也将无从谈起。拓竹使用安全启动，安全密钥管理，安全加解密引擎和可信执行环境等技术加固系统，跟上层软件紧密结合，从而最大程度上保护用户的隐私数据安全。

2.1.1 硬件可信环境

安全引擎和密钥管理

拓竹的所有 3D 打印机都使用了基于硬件的安全引擎，能够调用 OTP（One Time Program Area）中的密钥进行密码学运算，OTP 密钥写入后将被控制访问，从而避免密钥泄漏。X1 系列和 H2 系列的安全引擎支持 AES，SHA，RSA 等主流对称非对称算法和哈希算法。P系列和A系列支持 AES-XTS，HMAC，RSA 签名等常见算法。

同时，拓竹根据 NIST 建议 (https://www.keylength.com/en/compare) 选择合规算法、密钥强度和使用方式，如下表所示。

算法	强度（bits）	NIST建议	用途
AES	128	2030	加密
RSA	2048	2030	签名
ECC	256	2030	认证
ECDSA	256	2030	签名
SHA	256	2030	哈希

表1：NIST建议的推荐密码算法强度

可信执行环境

拓竹的 X1 系列和 H2 系列机型采用了 ARM® Cortex®-A 系列处理器，该系列处理器支持 ARM® TrustZone® 技术。这是一种可信执行环境（TEE）技术，它可以将处理器通过硬件划分为安全世界和普通世界。在拓竹的实现中，关键的安全功能如密钥管理，安全存储，固件解密验签等都是在安全世界里实现的，目的是通过可信执行环境来保证关键安全功能的完整性和密钥的机密性。

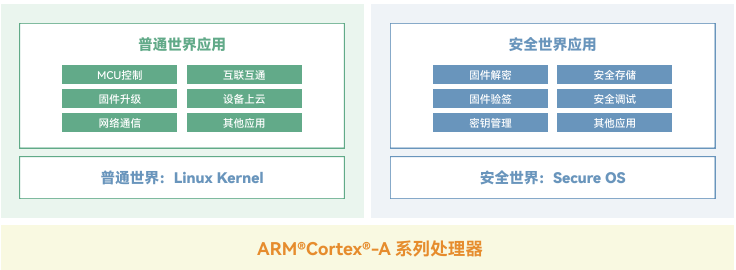

图2：普通世界和安全世界隔离

基于 RPMB 的安全存储

在拓竹的 X1 系列和 H2 系列机型支持基于重放保护内存块 (RPMB)，RPMB 是设备存储中的一个安全区域，它采用签名和重放保护机制，确保数据只能由 TEE 访问，并防止未经授权的访问。拓竹基于 RPMB 实现了安全存储功能， RPMB 里的数据在写入时经过加密，且只能通过TEE才能修改，从而使得一些重要的数据和标志位能够安全的记录下来，进而避免被攻击者恶意篡改关键数据，影响用户隐私和数据安全。

基于加密 Flash 的安全存储

在拓竹的 P1 系列和 A1 系列机型基于 flash 的 AES-XTS-256 透明加解密功能实现了安全存储功能，密钥存储在 Efuse 中只能通过硬件安全引擎读取和使用。加密后的 flash 分区能够避免攻击者通过磨片的方式获取 flash 上的明文数据，从而保护用户的隐私和数据安全。

设备证明

为了确保 3D 打印机的可信度，拓竹在每台打印机中都预装了设备证书，用于唯一标识每一台打印机。此类证书的公钥集中存储在拓竹的服务器中，私钥存储在设备上的安全存储里。在需要验证设备身份的场景中，设备可以向拓竹服务器发送身份验证请求，以验证设备的真实性。

2.1.2 安全启动

Secure Boot

拓竹所有机型都支持 Secure Boot，Secure Boo t功能的原理是利用设备启动时，处理器会执行存储在片上只读存储器中的 BootROM 代码。这段代码在制造过程中已固化到芯片中，无法篡改。BootROM 将验证存储在闪存中的二级引导加载程序。验证成功后，固件将被验签并加载。启动过程中的每一步经过验签，以确保启动过程中每个固件的完整性。

Verified Boot

拓竹的X系列和H系列机型还支持 Verified Boot 功能，Secure Boot 功能主要验证了启动固件的完整性，并不支持验证文件系统是否被篡改，而 Verified Boot 技术能够验证启动时挂载的 Systm 分区文件系统是否被篡改过。通过 Secure Boot，Verified Boot 功能组合，能够有效防御打印机上被安装恶意软件或 Rootkit 的情况。

文件系统加密

拓竹的 X1 系列和 H2 系列机型还支持文件系统加密功能，该功能主要被用于保护 System 分区的机密性，增加逆向分析难度。对攻击者来说，如果无法进行逆向分析，攻击门栏将显著提高，整体系统防御纵深因此得到加强，进而起到保护用户隐私数据安全的作用。

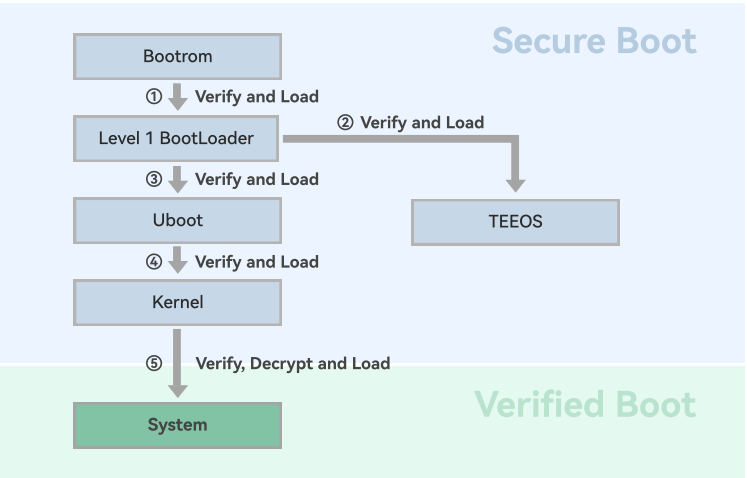

图3：X1系列和H2 系列 Secure Boot + Verified Boot

2.2 系统安全

如果说硬件安全是系统安全的基础，那么系统安全则是建立在坚实的硬件安全基础之上的重要屏障。它涵盖了操作系统、应用程序等多个方面，旨在通过各种软件机制来防范恶意软件的入侵、未授权的访问、以及数据泄露等安全威胁。

2.2.1 内核安全

强制访问控制

拓竹的高端机型支持强制访问控制功能。强制访问控制能通过预先定义和强制执行这些访问规则，为应用程序设置细粒度的安全策略，可以实现精确地控制每个应用程序能够访问的系统资源，例如文件系统、网络、设备以及其他的进程间通信接口。

通过使用强制访问控制措施，即使某个应用程序存在安全漏洞并被恶意利用，其能够造成的损害也会被严格限制在预设的范围之内。强制访问控制能提升设备整体的防御纵深，从而达到保障用户的隐私数据和使用安全的目的。当前该功能在 H2C 上支持，未来将拓展到 X1 系列和 H2 系列的其他机型上。

KASLR

拓竹的高端机型支持 KALSR（内核地址随机化）安全特性，KASLR 特性使得内核加载基地址每次都是随机的，使得攻击者无法简单获取内核地址布局信息，进而增加代码重用攻击的难度。代码重用攻击是现代攻击内核的常见攻击手法，使用 KASLR 特性能够有效提高内核安全性，进而起到保护用户隐私数据的作用。当前该功能在 H2C 上支持，未来将拓展到 X1 系列和 H2 系列的其他机型上。

2.2.2 安全升级

拓竹的 3D 打印机都支持远程升级功能，通常用于新功能发布，问题修复或安全补丁等场景。固件在拓竹开发测试完成后，经过加密和验签后上传到拓竹的固件服务器上。经过验证无误后，固件会在固件服务器上正式发布，用户可以通过 App 升级，或者通过下载到 SD 卡或 U 盘中对打印机进行离线升级。

图4：固件安全升级

固件签名密钥在拓竹内部严格保护。固件公钥的 Hash 在设备端存放在 Efuse 中，即使设备端被攻击者破解，也无法篡改公钥或获取私钥。在拓竹的高端机型中，设备端固件的解密和验签在 TEE 中进行，借助硬件基础设施进一步提高了攻击门栏。

固件加密和固件签名能够保证固件的机密性和完整性。固件加密可以增加逆向分析的难度，进而增加攻击门栏。固件签名可以防止被恶意篡改后的固件升级到用户的设备中，从而达到保护用户隐私数据的目的。

2.2.3 调试接口关闭

拓竹产品出厂时，JTAG、串口等调试方式均被禁用，避免了攻击者通过调试接口获取固件，篡改固件运行逻辑的情形。这增强了固件的安全性，有效防止打印机被入侵和用户数据泄露。

2.3 网络安全

拓竹的 3D 打印机其中一个核心特性便是通过网络连接至云服务。这一“上云”能力极大地拓展了用户的使用边界，实现了模型下发，发送打印任务、远程监控、接收固件更新、访问模型库等核心功能，为用户带来了前所未有的便利和效率。

然而，设备的网络连接性在带来便利的同时，也引入了潜在的安全风险。一旦设备暴露在不安全的网络环境中或其自身的网络防护存在漏洞，可能面临未经授权的访问、数据泄露、恶意控制甚至服务中断等威胁。因此，保障 3D 打印机设备端的网络安全至关重要。

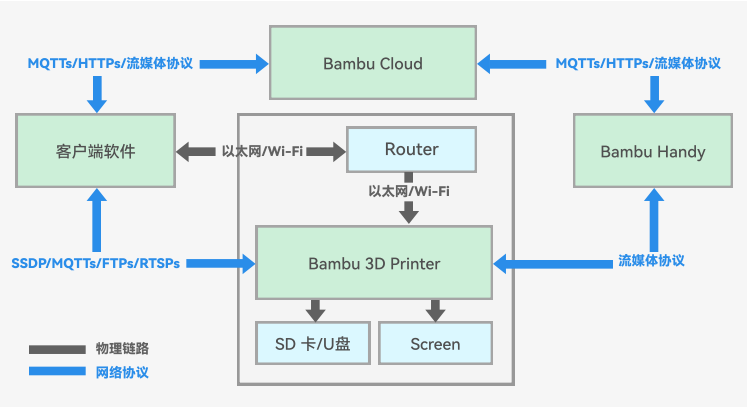

图5：拓竹3D打印机网络拓扑

2.3.1 安全网络协议

安全网络协议的实施可以降低用户设备连接到网络时数据泄露和篡改的风险。拓竹的 3D 打印机默认使用安全通信协议，包括 HTTPs，MQTTs，RTSPs，FTPs，DTLS 协议等。通信数据经过加密签名，对端身份经过验证，可以有效避免用户数据泄露风险。

拓竹的 3D 打印机的网络连接支持有线网络和 WiFi 连接，Wi-Fi 连接支持 Wi-Fi 安全协议，包括 WPA/WPA2-PSK。WPA2 对每个连接进行认证，并提供 128 位 AES 加密，以帮助确保在空中发送的数据的保密性。WPA2 是一个常用的加密协议，确保用户数据在通过 Wi-Fi 网络连接发送和接收通信时始终受到保护。

拓竹的企业机型（X1E和H2D Pro）还支持 WPA2-Enterprise，WPA2-Enterprise 提供了更高的安全性。通过实施个人用户身份验证、高级身份验证方法和加密，WPA2-Enterprise 有助于确保企业环境中无线通信的机密性、完整性和真实性。

拓竹P1系列支持蓝牙低功耗（BLE），用于通过 Handy 应用程序进行打印机网络配置和绑定，它利用 AES-CMAC 和 P-256 椭圆曲线，同时还使用 AES-CCM 协议来确保安全配对。

拓竹打印机也可以工作在局域网模式下，使打印机在不需要云端通信的情况下也能发挥作用。在局域网模式下对打印机的控制是通过本地部署的控制协议和部署在打印机内部的 MQTT 服务器进行的，默认使用 MQTTs 。文件传输使用 HTTPs，MQTTs，RTSPs，FTPs，DTLS 进行，可以实现安全的文件上传和下载。

2.3.2 设备上云

为了提供打印机的远程控制功能，拓竹采用物联网服务，包括设备登录、设备信息同步、固件/软件更新、用户设备绑定、远程打印、切片参数管理、云切片、故障检测等功能。

设备登录

每个设备都有一个独特的内置不少于 120 位 ID 和密码，这些都是在工厂随机生成的。当设备接入物联网时，云端和设备端会进行双向认证。设备端校验云服务身份，云服务校验设备端身份，设备端身份依赖设备生产时内置的公私钥对。只有双向认证通过，设备端才能接入物联网服务。双向认证后，云端会进一步校验设备真实性，避免设备中的公私钥对意外泄露后，在云端产生大量伪造设备的情况。

设备绑定

打印机可以通过以下 3 种方式连接到一个用户账户：

- 扫描打印机上显示的二维码（5分钟过期）
- 通过 SSDP 信息，通过局域网连接到打印机
- 通过蓝牙连接进行连接

这三种设备绑定方式都将通过安全的绑定协议进行绑定。

模型上传安全

G-code 可以使用局域网网络连接发送到打印机，如果有稳定的互联网连接，也可以通过我们的云服务发送到打印机。当文件通过我们的云服务发送到打印机时，G-code 文件会通过HTTPS安全通道发送到一个临时的私人存储位置。上传的文件包含有效期和相关的认证签名，并且只能用于上传，以最大限度地保证数据安全。

文件上传到云端后，打印机从 MQTT 打印命令中获得打印文件地址，下载到本地，并在开始打印过程前对其进行解析。用户可以在 Bambu Handy App 上进行隐私配置，

- 如果设置为无痕模式，云端临时存储的 G-code 文件会在 3 天后自动清除。
- 如果不设置无痕模式，临时文件将在 90 天后自动删除。用户在 90 天内可以在云端重新发起打印。

视频流服务安全

当涉及到视频流服务时，云连接作为一个安全中介，验证请求并向客戶端提供流。视频流和文件传输都有 TLS/DTLS 加密保护。在完成握手以授权数据流后，连接将在 Handy App/Studio 与打印机之间直接建立，完全绕过我们的服务器，从而确保端到端的隐私保护和最低延迟。

2.3.3 配件安全校验

3D打印机有许多配件，拓竹 3D 打印机主要设计为与拓竹原装的配件配合使用。根据配件功能的不同，对那些可能影响打印质量，可能损坏打印机，以及可能对用户人身财产造成安全的配件，我们会进行安全认证，避免可能产生风险的异常配件接入。

每个被认证的配件，内部都有一对唯一的公私钥对。跟 3D 打印机连接后，3D 打印机会通过challenge-response 的方式校验设备的真实性，从而确保关键配件不是异常配件。降低安全风险。

2.3.4 授权控制

3D 打印机暴露在网络环境中，有被攻击者远程攻击的风险。在我们持续运营的云服务中，也发现每天有海量来自非官方客户端的异常请求，严重威胁着服务可用性。因此，我们设计了授权控制功能，授权控制功能设计的设想是为拓竹 3D 打印机的连接和控制增加授权和身份验证保护机制，只有授权的访问和操作才能被允许，未授权的访问和操作将被禁止。

授权控制原理

授权控制功能是通过对控制打印机的关键控制命令进行鉴权来实现。打印机在执行关键控制命令前会验证关键控制命令的签名是否正确。正常情况下，Bambu Studio 会通过调用网络插件跟打印机通信。在授权控制功能使能后，网络插件将认证调用它的软件的身份（通过软件的签名，当前主要在 Windows 和 MacOS 上，Linux 平台暂不支持），只有经过身份验证的软件才能发起关键控制命令。这是因为网络插件内部内置了私钥，没有经过身份认证的软件发起的关键控制命令不会被签名，3D 打印机发现签名验证不通过时就不会执行该命令，从而达到授权的软件才能控制的目的。虽然内置的私钥虽然无法通过硬件保护，但是通过多种软件加固的方式相结合，依然能起到显著增加攻击者门槛的作用。

授权控制功能将限制三方软件直接不受控制的调用危险接口，但这同样将影响那些非恶意的软件接入拓竹的打印机。因此我们提供了 Bambu Connect 软件，该软件旨在提供一个集成了安全协议的，精简的用户界面，从而简化三方软件接入。通过 Bambu Connect 软件可以安全的进行发起打印的工作。Bambu Connect 也内置了私钥，并采取了跟网络插件相同的软件加固方式。也能起到提高攻击者门槛的作用。

局域网-开发者模式

在授权控制功能发布后，我们收到了广泛的反馈，许多打印农场主都对 3D 打印机的可靠和不间断访问表示担忧。我们理解这些企业面临的风险，虽然当时授权控制功能还在Beta阶段，但是依然可能对打印农场的设备或第三方软件使用者造成影响。因此，我们决定为局域网模式增加一个可选项：开发者模式。从而为高级用户提供更强大的控制力和灵活性。

在开发者模式下，打印机的 MQTTs 和 FTPs 将不受授权控制功能管控，三方软件可以正常工作。同时，用户也可以选择不升级，降级固件到授权控制版本使能之前，从而继续使用三方软件。关于开发者模式的试用可以参考以下链接：https://wiki.bambulab.com/zh/knowledge-sharing/enable-developer-mode

合作邮箱

如果您对授权控制功能有任何意见，或者您是第三方软件开发者，可以通过 devpartner@bambulab.com.邮箱沟通合作事宜。

2.4 隐私保护功能

我们深知用户对隐私和数据安全的重视。为此，我们不断倾听用户需求，持续优化产品功能。虽然用户的顾虑无法完全消除，但倾听和尊重始终是我们的选择，将用户的担忧转化为实际行动，力求在便捷性与隐私数据保护间实现平衡。目前，设备端为用户提供了以下几个隐私保护功能：

2.4.1 局域网模式

在 3D 打印机联网后，虽然给用户提供了更多方便，但也同时也给用户带来了更多隐私和数据安全上的顾虑。在听取用户反馈后，我们为有隐私和数据安全顾虑的用户提供了局域网模式。在局域网模式下，3D 打印机将不会对外发起连接，Bambu Handy 也将无法使用，客户端软件跟打印机在局域网里通信。在局域网模式下通信协议仍然使用安全的通信协议（MQTTs，FTPs，RTSPs 等），从而避免局域网里潜在的攻击者监听或篡改数据。

在局域网模式下，客户端软件通过输入设备的 PIN 码来跟设备绑定，设备绑定过程也只在局域网里进行，不需要连接服务器。设备绑定功能为设备提供了在局域网下的访问控制能力，能够避免相同局域网里潜在的恶意设备直接控制打印机，进而造成安全风险。

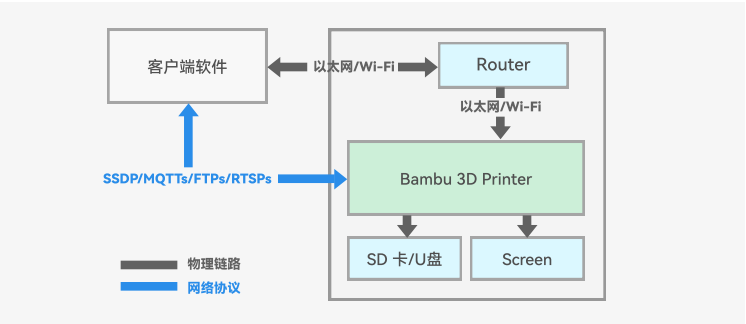

图6：局域网模式网络连接

通过使用局域网模式，可以使 3D 打印机的通信只在本地网络里传播，避免数据上传到互联网中，从而达到保护用户隐私和数据安全的目的。具体如何使能 LAN Only Mode 可以参考以下链接：https://wiki.bambulab.com/en/knowledge-sharing/enable-lan-mode

如果局域网模式仍然不能消除你的隐私安全顾虑，拓竹 3D 打印机也支持完全离线使用，用户可以选择关闭网络连接，从而进入完全离线的状态，然后使用 SD卡或 U 盘进行 3D 打印。

2.4.2 网络开关

X1E 和H2D Pro 支持网络开关功能，在 X1E 上，可以通过网络开关关闭有线网络和无线网络，从而避免数据流出。H2D Pro 该功能进行了优化，网络开关支持通过网络开关通过下电的方式彻底关闭无线网络，用户可以通过不插网线的方式关闭有线网络。通过网络开关功能，能够让企业机型能够安全的工作在用户的环境中，满足企业用户的隐私安全要求。

2.4.3 离线升级

局域网模式下虽然保证了数据不会流出局域网，但是也限制了原本需要联网的功能的可用性，包括最初的升级功能。用户在局域网模式下无法更新固件，联网更新固件就破坏了原本的隐私和数据安全设置。在听取了用户反馈后，我们决定为用户提供了离线升级功能，让用户在局域网模式下依然能通过 SD 卡更新固件。

图7：离线升级

通过离线升级功能，能让有隐私数据安全顾虑的用户在既能保证原有的隐私和数据安全设置的情况下，也能正常使用最新的固件功能。

2.4.4 日志导出加密

日志导出加密功能，最初是为了防御网络攻击，保护用户隐私的目的设计的。一方面可以在未授权访问的场景下避免潜在风险人员直接获取用户设备的明文日志信息，从而起到保护用户隐私数据安全的作用。另一方面，日志中包含的一些信息直接明文导出也会带来网络安全风险，比如内核日志中包含的地址信息可能被攻击者用来绕过 KASLR 等内核安全保护，显著提高代码重用攻击的风险。

但是日志加密也意味着用户并不知道到底给拓竹提交了哪些数据，这曾给我们带来了一些毫无根据的严重指控，并在社区造成了强烈反响。哪怕这些指控的基本事实是错误的。当然，这背后的真实原因是日志加密后对用户缺乏透明性，才让无端指控在猜疑下拥有了发挥的土壤。

这些事情发生后，我们决定给日志导出增加更多的透明性，让保护网络安全，保护用户隐私和给用户透明性之间取得一定的平衡。当前，虽然日志在导出时依然会被AES算法加密。但是我们给用户增加了导出数据的说明和选项，让用户能够根据自己的实际情况决定导出哪些数据给我们。

拓竹的 X1 系列和 H2 系列支持通过 SD卡 导出日志，其中 X1 系列支持 AES128 的日志加密，H2 系列支持 AES256 的日志加密。高端机型系列支持导出的数据主要有三类：系统日志，传感器数据和 G-code。其中传感器数据和 G-code 是否导出是用户可选的，传感器属于有助于判断激光雷达和炒面检测相关问题，G-code 有助于判断打印质量问题。用户可以根据自己的实际情况选择是否导出。

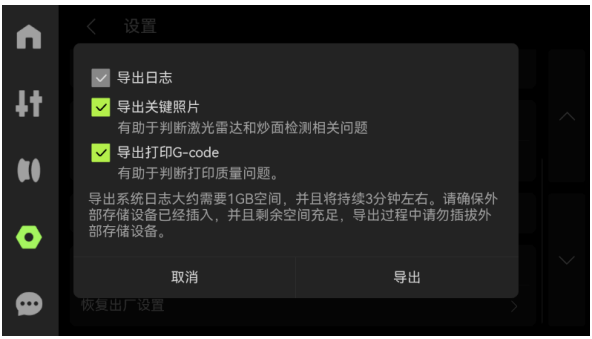

图8：日志导出选项

在拓竹 P1 系列和 A1 系列中，日志默认加密并存储在 SD 卡中，日志大致用途如下，用户可按需提交相关日志。

- **logger:** 提供简明的打印流程日志，所有问题的排查都需参考该文件夹中的日志。
- **recorder:** 用于定位调平校准异常、打印质量问题、传感器异常导致的打印停止、打印失败，以及打印过程中异常停止等问题的关键日志。
- **corelogger:** 记录系统异常时的状态信息，用于诊断打印异常停止问题。

拓竹所有机型的打印机，日志导出功能完全由用户发起，除非用户主动上传，否则拓竹将无法接触到用户的日志数据，用户上传的日志，在工单处理完成 14 天后将被自动删除。具体日志加密导出和上传功能可以参考：https://wiki.bambulab.com/zh/X1/troubleshooting/how-to-upload-log

2.4.5 恢复出厂设置

拓竹的 3D 打印机支持恢复出厂设置功能，一旦进行恢复出厂设置，用户的配置数据将被重置。针对拓竹 X1 系列和 H2 系列，日志数据默认存储在设备内，恢复出厂设置时日志数据也会被清除。对于拓竹 P1系列和 A1 系列，日志数据默认存储在 SD 里，用户可以通过格式化 SD 卡的方式清除日志。

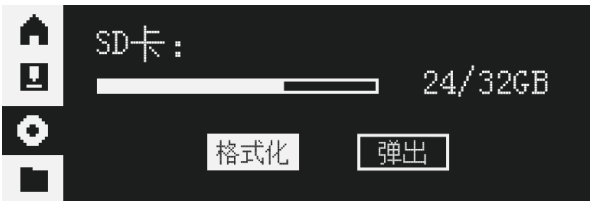

图9：P1 系列格式化 SD 卡

2.4.6 改进计划开关

在设备上，用户可以通过 设置 > 设备和 SN > 用户体验计划 来打开和关闭设备端的用户体验计划。用户体验改进计划是为了持续优化和提升用户的产品使用体验而设计的。该数据主要包含设备状态和使用情况的数据，用于分析和改善产品的体验。该数据经过加密后通过安全的通信链路上传，不会被第三方获取。

03 软件安全

在拓竹的产品服务生态中，软件扮演着至关重要的桥梁角色，涵盖了模型切片与编辑的 Bambu Studio 和 Bambu Suite，实现设备互联互通的 Bambu 网络插件和 Bambu Connect 组件，便捷移动操控的 Bambu Handy App，以及高效管理打印集群的 Bambu 农场管家等。无论是连接打印机、接入云服务、处理模型数据，还是实现农场设备的集中控制，都离不开这些软件的精密运作。它们是构建流畅、高效 3D 打印体验的关键基石。

这些软件工作在用户的 PC 或手机上，其安全性直接关系到用户设备、隐私数据乃至整个 3D 打印生态系统的安全。一旦软件层面存在安全漏洞，例如代码缺陷、配置不当或缺乏必要的安全防护，就可能成为黑客攻击的入口。被恶意重打包的软件也有可能被植入木马，导致用户的设计文件被窃取、打印机被恶意控制、个人信息泄露，甚至可能危及用户的网络环境安全。

因此，对这些软件进行全面的安全加固和签名非常重要，只有软件的安全性和完整性得到保证，才能确保拓竹产品服务的稳定可靠运行，进而保护用户的资产和隐私安全。

然而，我们也清醒地认识到，没有任何软件能够达到绝对的百分之百安全，特别是工作在不安全环境下的软件，训练有素的攻击者在持续投入的情况最终一定能完成攻击。这是一个动态的攻防博弈过程。尽管如此，我们坚定地通过采用多层次的安全加固技术和严密的软件完整性保护机制，来显著提升潜在攻击者的攻击门槛和成本。

拓竹始终在持续改进和更新软件，以应对不断涌现的新型安全威胁。同时，我们也强调，用户应及时将设备与软件升级至最新版本，以获得最高等级的安全保障。

3.1 软件加固

软件加固的目的是为了防止软件被逆向分析或重新打包后植入恶意代码，提升攻击者者的攻击门栏。拓竹的软件虽然工作在不同平台上（Windows，Linux，MacOS，iOS，Android），但是统一采用了下面几种软件加固手段:

3.1.1 软件 & App 签名

拓竹的 Bambu Handy App，已登陆 iOS 平台的 App Store，供用户便捷下载。能够上架 App Store，本身就意味着该应用通过了苹果公司严苛的安全审核流程。用户安装 App 时 iOS 系统将会校验 App 的签名，从而保证 App 未经第三方恶意篡改。

安卓平台的 Bambu Handy App 同样经过严谨的签名流程，并已在 Google Play 商店开放下载。与 iOS 平台类似，上架 Google Play 亦需通过其严格的安全检测。您的安卓手机在安装 App 时，也会对该签名进行核验，确证软件的完整性。使用应用商店版本或从 Bambu Lab 官网下载的安装文件可以有效避免下载到恶意应用。

不仅如此，拓竹的PC端软件（Bambu Studio，Bambu Suite，Bambu Studio网络插件，Bambu Connect），无论是 Windows 还是 macOS 版本都进行了数字签名。当您在操作系统中运行这些软件时，系统会清晰地提示您该软件是否由拓竹官方签名发布，有效警示潜在的仿冒或恶意程序。

此外，在 Windows 和 macOS 平台上，Bambu Studio 网络插件会校验调用网络插件的软件的应用签名，避免非授权程序直接使用 Bambu Studio 网络插件库跟打印机通信。

3.1.2 虚拟机保护

虚拟机保护是软件反编译领域的一种较为成熟的手段，其核心在于将可执行程序的原生机器码巧妙地转换为一套全新的、自定义的字节码或指令集。这些指令并非直接在底层硬件上执行，而是在一个精心设计的、软件实现的虚拟机环境中运行。原生机器码的语义被映射到这套全新的、鲜为人知的虚拟机指令上。要理解和还原程序的真实逻辑，攻击者不仅需要具备常规的反汇编和逆向工程技能，更艰巨的挑战在于必须先彻底逆向分析整个虚拟机的架构、指令集及其执行流程。 虽然虚拟机保护并非绝对无法攻破，但其显著地提升了逆向工程的复杂度和时间成本，极大地增加了攻击门槛。

拓竹的 App 和 PC 软件中，都统一使用了虚拟机保护技术，以固守软件内的关键资产，例如连接云端的认证令牌，以及与打印机通信时的认证消息签名密钥等核心凭证。我们也清醒地认识到，面对经验丰富的攻击者，即使是通过虚拟机保护的资产也不是 100% 安全。因此，我们的整体安全方案并非完全依赖这些敏感信息的绝对不泄露，而是将虚拟机保护作为提升攻击门槛的关键一环，通过显著增加攻击难度来降低被攻击的风险。

3.1.3 代码混淆

代码混淆也是业界对抗反编译的一种常见手段，其核心思想在于通过各种变换技巧，使得程序的源代码或中间代码变得难以理解和分析，但在功能上保持不变。相比虚拟机保护，代码混淆的强度更低，但是系统开销也更小。

拓竹的 App 和 PC 软件中，也统一使用了代码混淆技术，虚拟机保护通常用于保护核心资产和关键逻辑，代码混淆则通常用于非核心资产和关键逻辑的保护。代码混淆虽然无法阻止专业黑客的逆向分析，但是也能一定程度上提升攻击门栏，从而降低安全风险。

3.1.4 反调试

反调试技术主要用于防止软件被动态调试，虚拟机保护和代码混淆都能对抗静态分析，但是对训练有素的攻击者来说，常常是动态调试和静态分析相结合来分析，最终完成攻击。反调试技术主要针对的就是动态调试的场景。

拓竹的 App 和 PC 软件，也统一使用了反调试技术，通过反调试技术虽然同样无法阻止专业黑客的逆向分析，但依然能够增加动态调试的攻击门栏，进而降低安全风险。

3.1.5 关键资源加密

关键资源加密是通过加密的方式保护应用的关键资源。在上述保护的基础上，对运行时可能要使用或加载的关键资源文件使用标准的算法进行加密，运行时再解密，从而起到保护关键资源，减少关键资源泄露的风险。

3.2 应用程序隐私保护

应用程序运行在用户的 PC 或手机上，这意味着它会与用户的设备和数据进行交互。因此，我们非常谨慎地申请有用户权限，确保用户隐私得到充分保护。

3.2.1 Bambu Handy 隐私权限

Bambu Handy 应用程序在设计时遵循权限最小化原则，只会申请合理的权限。其中对可关闭的权限，用户可通过所用设备的设置功能单独关闭，申请这些权限的原因如下：

- **STORAGE** - 上传/更新账号头像、图文/视频内容的评论
- **CAMERA** - 使用设置或更新头像、相册管理、图像保存、视频录制、扫一扫
- **LOCATION** - 对智能设备配网时
- **NOTIFICATION** - APP相关消息推送
- **INTERNET** - 开启上网功能，设备配网功能等
- **BLUETOOTH** - 蓝牙设备配网时

3.2.2 Bambu Handy 隐私设置

Bambu Handy 应用程序为用户提供了隐私偏好设置功能，可以通过 “我的” > “设置” > “隐私设置” 进行配置。

无痕打印设置

Bambu Handy 支持无痕打印设置，开启无痕打印设置后，将不在 Bambu Cloud 服务器保存您的打印文件，当前无痕打印设置主要有以下三种选项，用户可以根据自己的隐私偏好进行选择：

- **不使用无痕打印** - 您可以从打印历史中发起打印
- **启用（有历史记录）** - 创建历史记录，但不在 Bambu Cloud 服务器上保存你的打印文件
- **启用（无历史记录）** - 不创建历史记录，也不在 Bambu Cloud 服务器上保存您的打印文件

浏览历史设置

Bambu Handy 支持浏览历史设置，主要有以下两种选项：

- **启用浏览历史** - 保存您在过去 7 天内查看过的模型，方便回溯足迹，提供更精准的个性化推荐。
- **禁用浏览历史** - 关闭浏览历史后，浏览历史不记录，您将无法轻松找到自己浏览过的模型。

3.2.3 Bambu Studio 用户体验改进计划

Bambu Studio的用户体验改进计划是为了持续优化和提升用户的产品使用体验而设计的。该数据主要包含设备状态和使用情况的数据，用于分析和改善产品的体验。该数据经过加密后通过安全的通信链路上传，不会被第三方获取。用户在授权后也可以自由关闭。

Bambu Studio 可以通过 偏好设置 > 用户体验 中选择是否加入该计划或撤回授权。

04 云服务安全

在拓竹的产品服务生态中，云服务是连接用户与设备、软件与平台的关键纽带。依托云端，用户能够简单的选择喜欢的模型，能够轻易的发起打印，远程监控和管理打印进度等。云服务极大地丰富了 3D 打印的使用场景与价值，但同时也带来了对数据安全和隐私保护的更高挑战。

与单一设备或本地软件不同，云服务需要承载海量用户数据的集中存储与处理，其中不仅包括用户的设计模型、打印参数和使用记录，还可能涉及敏感的商业信息与个人隐私。一旦发生未授权访问、数据泄露或服务中断，将对用户的知识产权、业务连续性乃至个人安全造成不可估量的影响。因此，云服务安全性不仅是拓竹构建数字化生态的基础，更是赢得用户长期信任的前提。

4.1 多层安全防护

为了确保云服务的安全性，拓竹为云服务（包括 Bambu Cloud Service，MakerWorld 等）添加了多层安全防护机制，如下图所示，一个网络请求在到达后端服务之前会将通过包括 CDN，DDoS 保护，Web 应用防火墙（WAF）等防护机制。

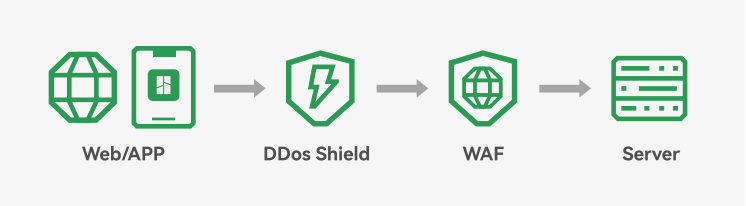

图10：多层安全防护

拓竹的云服务使用安全的通信协议，包括 HTTPs，MQTTs，RTSPs 等，确保通信过程不会被三方窃听。

云计算服务所使用的基础设施，拓竹将海外用户数据托管于亚马逊 AWS（美国），将中国用户数据托管在阿里云（中国）。AWS 和阿里云都通过了 ISO 27001/27017/27018/27018/27701，SOC2 等认证。拓竹也于 2025 年 4 月 11 日通过了 ISO:IEC 27001 和 ISO:IEC 27701 认证。

拓竹在全球化安全与加速方面采用了 Cloudflare 的服务。作为独立的边缘网络安全提供商，Cloudflare 在全球数百个节点为用户与拓竹云平台之间构建了安全的前置防护层，既提升了跨区域访问的速度与稳定性，也提供了高效的 Web 应用防火墙（WAF）和 DDoS 攻击防护。通过智能流量分析、实时规则拦截与大规模流量清洗，Cloudflare 有效防范了常见应用层攻击与大规模拒绝服务攻击，同时借助端到端加密保障用户数据传输的隐私与完整性，为全球用户带来一致、安全、可靠的云服务体验。

在中国大陆地区，除了使用 Cloudflare 服务，也使用了阿里云提供的 WAF 和 DDoS 攻击防护，Cloudflare 与阿里云的结合，使拓竹的云服务在全球范围内兼具国际化的性能与安全优势，以及在本地化运营中对合规性与安全性的双重保障。

云服务的运营和维护由拓竹的专业运营团队负责。遵循 Amazon AWS 和阿里云推荐的资源管理和安全配置最佳实践，遵循 Need-to-Know 和最小授权原则。在服务器端执行的所有权限和操作均受到严格的标准操作规程 (SOP) 的限制，并具有控制和审计机制。

4.2 Bambu 账号

Bambu 账号是用于识别拓竹用户的账户，用户可以通过该账号访问拓竹的产品和服务。拓竹非常注重用户数据的安全保护，为了保护用户账户，拓竹实施了多种登录保护措施来保护用户账户的数据安全。

4.2.1 登录方式

Bambu 账户登录支持两种登录方式，分别是账号密码登录和第三方账号绑定。

账号密码登录
在中国大陆地区，用户可以通过手机号和验证码，或者手机号和密码登录账号。在其他地区，用户可以通过邮箱和密码登录。用户在 Bambu Studio 可以通过 偏好设置 > 登录区域来切换登录区域。

第三方账号登录
Bambu 帐号支持关联第三方帐号授权，即用户可以使用第三方帐号登录 Bambu 帐号。目前，国内用户可以通过 Apple、微信，微博和 QQ 帐号关联 Bambu 帐号。 海外用户可以通过 Apple 账户，Google 账户，Meta 账户关联 Bambu 账户。Bambu 账号采用 OAuth2.0（开放授权协议），遵循 OAuth2.0 标准的协议和流程授权第三方帐号登录。OAuth2.0 的安全机制确保 Bambu 帐号信息不会被泄露给第三方。

4.2.2 登录保护

Bambu 账户当前为用户提供了以下两种登录保护措施，分别是双因子认证和一键注销账号。

双因子认证（异常登录）
当用户使用账号密码在新设备上首次登录 bambu 账号时，需要经过双因子认证才能登录。通过该机制能够有效防止用户账号密码泄露导致用户隐私数据泄露的情况。

一键登出账号
如果用户选择登出账号，在账号注销时会同步注销之前各客户端的登录态授权，从而减少用户账号数据泄露的风险。

4.2.3 数据安全

Bambu 账号的数据安全保护措施

在用户注册 Bambu 账号时，用户所填写的个人信息将会被加密和严格保护，以确保数据在存储与传输过程中不被泄露或滥用。

1.个人信息加密存储

- 手机号或邮箱：在写入数据库前，会使用 AES-128 对称加密算法进行加密存储，避免信息在数据库泄露时被直接读取。
- 密码：密码不会以明文形式保存，而是采用业界推荐的 Argon2 密码哈希算法进行不可逆处理，并在哈希过程中引入随机盐值，以有效抵御彩虹表攻击和暴力破解。

2.密钥管理与保护

- 所有加密操作所使用的密钥均由 KMS 统一管理。
- KMS 提供安全的密钥存储和操作，确保密钥不会以明文形式暴露给应用层。
- 系统会进行 密钥的定期轮换，并在发生潜在风险时支持紧急更换，进一步降低密钥泄露所带来的影响。

3.访问控制与最小权限原则

- 数据访问采用 严格的权限控制策略，仅允许经授权的服务或人员在必要时访问相应数据。
- 系统内部采用 最小权限原则，确保每个模块或员工只能访问完成其任务所需的最小数据范围。
- 所有数据访问操作都会被记录在 审计日志中，并由安全团队定期审查。

4.安全测试与合规

- 内部有专门的安全团队，持续开展 自动化安全检测与渗透测试，对系统可能存在的安全漏洞进行提前发现与修复。
- 除了内部测试外，还会定期邀请 第三方安全机构进行独立的外部渗透测试和安全评估，以确保系统符合行业安全标准。
- 系统在设计与运营过程中会参考并遵循 ISO/IEC 27001、GDPR 等国际安全与隐私保护标准，为用户提供合规的数据保护。

5.传输安全与实时防护

- 用户与云服务之间的通信采用 TLS 1.2 及以上 加密传输，防止中间人攻击和数据窃听。
- 平台部署了 实时入侵检测与防护系统（IDS/IPS），能够在发现异常行为或攻击迹象时自动响应，降低潜在风险。

4.3 MakerWorld 内容安全

4.3.1 内容审查规则

竹为 MakerWorld 实施了全面的内容安全检查，以确保平台安全且尊重用户。此审查流程涵盖各类被禁止的内容和行为。

MakerWorld 内容安全审查重点领域如下：

- **垃圾邮件和欺诈行为**：包括虚假参与、冒充、重复内容和诈骗。该平台旨在防止误导性信息和知识产权风险，例如使用不正确或不相关的源模型链接、购物网站或其他用户模型的图片。
- **敏感内容**： MakerWorld 禁止危害儿童安全的内容、缩略图中的露骨或敏感图像、裸体和性内容、与自杀和自残相关的内容以及粗俗语言。
- **暴力或危险内容**：此类别涵盖骚扰和网络欺凌、有害或危险内容、恐怖主义和极端主义言论、暴力犯罪组织的内容以及模特列表、帖子或评论中的暴力或图形内容。
- **攻击性言论**：禁止的攻击性言论包括辱骂或诽谤其他平台、使用粗俗或淫秽语言、骚扰、欺凌、人身攻击、对国家或民族进行有害诽谤、煽动种族或民族仇恨、威胁使用暴力或伤害、以及宣扬歧视或不容忍的仇恨言论或行为。
- **管制商品**： MakerWorld 禁止销售可变成枪支或爆炸物的模型（道具或玩具除外）、非法模型或物品以及宣传非法或管制商品、服务或交易的内容。

违反这些准则会导致违规内容被删除。此外，拓竹还对印刷版个人资料的投稿引入了更严格的准则，要求上传已完成印刷的真实照片，以确保质量，并防止上传存在明显质量问题或不匹配的个人资料。

4.3.2 知识产权规则

MakerWorld 是一个鼓励创作者自由分享的社区，同时也高度重视知识产权保护。拓竹为此制定并实施了严格的知识产权管理规范。规则如下：

类别	规则内容	说明
必须上传合法内容	仅允许上传原创或已获得授权的模型	上传者需拥有版权、使用权或授权许可
不得侵犯知识产权	禁止上传侵犯版权、商标、专利等内容	上传该类模型将导致下架、扣分或封号
必须正确归类模型	模型应明确标注为“原创”或“Remix”	错误分类将导致下架、扣分或封号
不得误用 Remix 标签	轻微修改如缩放、修复不应标记为 Remix	仅有实质改动才可作为 Remix 上传
必须遵守原始许可条款	遵循原模型的开源协议限制	如 CC-BY 需署名、CC-BY-ND 禁止改编等
必须提供打印证明（如标 CC0）	上传 CC0 模型时须附真实打印照片	用以验证模型可打印性，防止滥用 CC0

表2：知识产权规则

他人举报或平台发现可触发模型下架

- 社区成员可以举报涉嫌侵权的模型；
- MakerWorld 有权在无需通知的情况下，删除相关内容并对用户进行处罚。

更多社区规则详细信息，可以参考MakerWorld官方社区指南：https://makerworld.com/en/community-guidelines

05 隐私合规

在拓竹，我们深知用户对隐私的珍视与日俱增。尊重并保护每一位用户的个人信息，是拓竹运营的基石，也是我们构建长期信任关系的首要原则。为了将这一承诺落到实处，我们不仅以开放合作的态度不断听取用户反馈改进产品，也在组织层面设立了专门的安全委员会，致力于构建和完善全面的拓竹产品安全和隐私保护体系。更积极寻求国际权威机构的认可。通过一系列严谨的评估与审核，我们成功获得了多项国际隐私与安全认证，这不仅是对我们现有实践的有力证明，更彰显了我们持续提升隐私保护水平的坚定决心。

5.1 隐私安全认证

拓竹获得全球认可的信息安全和隐私认证，彰显了我们在维护国际公认的安全和隐私标准方面的领导地位

以下是我们信息安全和数据隐私认证的部分列表：

5.1.1 ISO/IEC 27001

拓竹已经于 2025 年 4 月 11 日通过 ISO/IEC 27001 认证，ISO/IEC 27001 标准已成为全球广泛认可且严格的信息安全管理标准，此次认证标志着拓竹履行了对用户的承诺，符合国际标准的要求。

Certificate no.: 763240-2025-AIS-RGC-UKAS
Place and date: Shanghai, 11 April 2025

5.1.2 ISO/IEC 27701

拓竹已经于 2025 年 4 月 11 日通过 ISO/IEC 27701认证，ISO/IEC 27701:2019 是专为隐私保护而制定的最新国际标准，将隐私保护实践纳入信息安全管理体系。此次认证表明拓竹坚持最佳的隐私保护实践。

Certificate no.: C763239
Place and date: Shanghai, 11 April 2025

5.1.3 TrustArc Enterprise Privacy

TRUSTe 认证是由 TrustArc 制定的隐私与数据治理框架，该机构专注于隐私保护领域的认证工作。拓竹已经于 2025 年 7 月获得该认证，获得该认证表明拓竹已经建立并实施了一套符合国际标准的隐私合规管理体系。

5.2 隐私实践

5.2.1 隐私处理原则

在拓竹，我们的产品和服务基于以下四项基本隐私原则。

隐私原则	描述
公开透明	我们努力使我们的数据处理实践保持公开透明，以便您做出明智的选择
开放合作	我们努力听取用户反馈，发觉其中的隐私安全改进点，并在产品和服务中不断改进
用户可控	我们力求为用户提供简单易用的方法来帮助用户控制自己的信息
隐私合规	我们的隐私实践严格遵从当前隐私和数据安全法律和标准，并通过相关认证

表3：隐私处理原则

5.2.2 隐私政策

拓竹高度重视用户隐私。我们的《隐私政策》详细阐述了我们在收集、使用、披露、处理和保护您在使用拓竹产品或服务过程中所提供的或我们收集到的个人信息方面的具体实践。我们承诺以透明和负责任的方式对待您的数据，并采取符合行业最佳实践的技术和组织措施来保护您的信息安全。为了更全面地了解我们的隐私保护措施，请您务必查阅我们的官方《隐私政策》：https://bambulab.com/en/policies/privacy。

5.2.3 数据存储策略

拓竹充分考虑到全球不同地区的数据保护法规和用户需求，采取了灵活且安全的全球数据存储策略。目前，用户数据的存储位置主要取决于用户所在的地理区域。具体而言：

- **中国大陆地区用户数据：** 用户的个人数据将存储在中国大陆境内的阿里云上，并遵守中国相关的法律法规。
- **其他地区用户数据：** 位于中国大陆以外地区的用户数据，当前会存储在位于美国 AWS 上的数据中心，并实施严格的数据访问控制和加密措施，以确保数据的安全性。

未来，随着业务的拓展和各地法规的变化，我们可能会对数据存储位置进行调整，但任何调整都将符合当地的法律法规要求，并会及时通知用户。我们致力于为全球用户提供安全可靠的数据存储服务。

如果您对隐私方面有任何疑问，请通过 privacy@bambulab.com 与我们联系

06 开源计划

如果说过去十年，谁是3D打印领域真正的英雄，真正的英雄应该是那些在Reprap、Marlin、Cura、Prusa、Slic3r、Hypercube、Voron 和 Klipper 背后的人，正是 3D 打印社区的开放性推动了桌面 3D 打印的发展。拓竹作为 3D 打印的后起之秀，我们从前辈那里学到了很多很多，站在巨人的肩上让我们有了快速发展的机会。

正因为我们从社区中学到了很多，我们始终对 3D 打印开源社区以及整个软件开源社区保持敬意，因此：

- 对我们产品中使用到的开源代码，我们严格遵守开源协议进行了开源

  开源地址：https://wiki.bambulab.com/en/knowledge-sharing/open-source-software

- 我们对切片软件做了大量的修改，添加了一些新的算法和技巧，增加了项目管理器和简洁的用户界面，作为我们对社区的一点回馈。

  开源项目网址：https://github.com/bambulab/BambuStudio

拓竹未来也将严格遵守开源协议，持续回馈社区。期待未来能与更多的开发者和爱好者携手前行，推动 3D 打印技术的进步。

07 漏洞赏金计划

拓竹漏洞赏金计划是邀请安全专家识别拓竹产品和平台的安全漏洞，并由拓竹给予安全专家相应赏金的项目。这个项目也是拓竹秉持开放合作的态度，跟业界建立公开合作以持续提升产品安全和数据隐私保护计划的一部分。

项目运作两年多的时间里，共有 51 位安全专家参与了该项目，截至目前，我们已经累积送出几万美元的赏金和多台打印机设备作为奖励。我们衷心感谢这些安全专家为拓竹不断改进产品安全和用户隐私上做出的努力。我们深知，保障 3D 打印机的产品安全和生态安全离不开跟安全社区的持续投入和通力合作。

有关该计划和赏金的详细信息，请参考：https://bambulab.com/en/security 如果您对该计划有什么建议，也可以通过security@bambulab.com 邮箱来反馈。

08 结论

拓竹致力于为全球个人、创客及行业用户提供创新、高效、安全的 3D 打印设备及解决方案。作为拓竹产品体验的核心组成部分，我们的固件，软件和服务肩负着构建用户信任、保障设备与数据安全的重要责任。拓竹将持续精进安全技术，增强产品和服务的安全与隐私保护功能，并不断优化我们的安全与隐私管理体系。我们将通过技术文档、白皮书、隐私政策，安全审计&认证等多种途径，向用户清晰地展示我们的安全实践与承诺，助力用户建立对拓竹产品和服务的信心，从而更加安心地选择和使用我们的创新技术。

我们坚信，只有对用户数据安全和隐私的充分尊重与保护，才能赢得用户持久的信任。我们将持续加大在该领域的投入，以开放合作的态度跟安全社区通力合作提升产品和服务的安全性，以倾听和尊重的态度认真听取用户反馈，更重要的是，我们不会止步于倾听，而是将用户的担忧转化为实际行动，融入到产品改进的每一个环节，唯有切实的努力和持续的优化，才能逐步赢得用户的信任。