Fleet Hub Security White Paper EN v1.0

1. Introduction

Fleet Hub is a printer control access box purpose-built for third-party system integration. While providing standardized RESTful API interfaces, it embeds layered security controls into every level of its system architecture. We understand that for service providers and software developers integrating printing capabilities into their platforms, security is not optional—it is a fundamental design requirement.

This white paper provides a comprehensive overview of Fleet Hub's security architecture and technical implementation, helping partners and developers evaluate and understand the measures we have put in place. For any security-related questions or feedback, please contact: security@bambulab.com.

2. Hardware Security Infrastructure

Fleet Hub’s security architecture is anchored in hardware-based trust roots. The following mechanisms provide tamper-resistant protection for cryptographic keys, firmware integrity, and runtime operations, establishing a hardware-enforced root of trust (HRoT) for the entire software stack.

Figure 1: ***Fleet Hub Hardware Form Factor***

- **Secure Boot:** Fleet Hub supports hardware-based Secure Boot, ensuring that every firmware component loaded during the boot process is officially signed by Bambu Lab. This prevents unauthorized or malicious firmware from running on the device.
- **Trusted Execution Environment (TEE):** The TEE provides a hardware-isolated secure execution environment. Critical authentication logic and cryptographic operations run inside the TEE, isolated from the general operating system. Even if the system layer is compromised, operations within the TEE remain hardware-protected.
- **Hardware Security Engine:** Fleet Hub integrates a dedicated hardware cryptographic engine supporting mainstream algorithms including AES, RSA, ECDSA, and SHA. This accelerates cryptographic operations while significantly reducing the risk of key material being extracted through software-layer attacks.
- **Secure Storage (RPMB):** By combining the Replay Protected Memory Block (RPMB) with the TEE, Fleet Hub implements secure storage for critical assets such as device certificates and password hashes. RPMB is a protected partition within the storage device that uses signature and replay-protection mechanisms to ensure data can only be accessed by the TEE, preventing unauthorized reads or writes.
- **Hardware Key Ladder:** Firmware used during boot and runtime is encrypted. The encryption keys are protected by a hardware Key Ladder mechanism—a hierarchical key derivation scheme in which the root key is permanently embedded in hardware and derived keys are generated transiently during operation. No software component can retrieve the plaintext key at any stage.
- **Efuse(OTP):** The trust root, firmware signing public key hash, and other critical configuration data are stored in eFuse — a one-time programmable area within the chip that is hardware-enforced and cannot be modified by any software means after programming.
- **Debug Interfaces Disabled by Default:** Hardware debug interfaces such as JTAG and SWD are permanently disabled via eFuse at the time of manufacture and cannot be re-enabled.

These mechanisms operate as an interdependent trust chain. The eFuse stores hardware-enforced verification key hash for Secure Boot; Secure Boot validates firmware integrity before execution; the Key Ladder decrypts firmware without exposing keys to software; the TEE isolates runtime secrets from a potentially compromised Rich OS; RPMB secures persistent credentials via TEE-mediated access. Together, these controls significantly raise the cost, complexity, and skill required to execute a successful attack against the platform.

3. System Security

Fleet Hub’s system security architecture extends hardware trust roots into the software stack through layered defense-in-depth controls. Operating under secure-by-default policies with mandatory privilege isolation, the design goal is not only to prevent initial compromise, but to contain the impact of any single exploited component and make lateral movement across security boundaries extremely difficult.

- **Verified Boot and Filesystem Encryption:** Secure Boot protects the integrity of the boot chain, while Verified Boot extends that protection upward—verifying the integrity of filesystem partitions at startup to ensure the operating system environment itself has not been tampered with. Together, they provide an unbroken integrity chain from firmware to the running OS. Fleet Hub also enables filesystem encryption on critical system partitions, meaning that even if an attacker physically reads the storage chip directly ("dump flash"), they will only obtain encrypted data that cannot be reconstructed into usable firmware or system content.
- **Mandatory Access Control (MAC):** Fleet Hub enables a mandatory access control mechanism at the OS level. Unlike traditional discretionary access control, MAC enforces security policy centrally—each application can only access the system resources it has been explicitly authorized to use, and cannot escalate its own privileges or access data belonging to other components. Even if a component is exploited, the attacker's operational scope is strictly constrained to that component's permission boundary, effectively preventing a single breach from becoming full system control.
- **Kernel Security Hardening:** Fleet Hub enables multiple kernel security mechanisms. KASLR (Kernel Address Space Layout Randomization) randomizes the memory base address at which the kernel loads on each boot, preventing attackers from predetermining the location of critical kernel functions and significantly raising the bar for code-reuse attacks such as ROP (Return-Oriented Programming). Access to high-risk kernel interfaces such as `/dev/mem` is also restricted, reducing the possibility of attackers directly reading or writing physical memory through these interfaces.
- **Firmware Encryption and Offline Secure Upgrade:** Firmware released for Fleet Hub undergoes both encryption and signing. Firmware encryption increases the difficulty of reverse engineering, making it harder for attackers to extract information or identify exploitable vulnerabilities. Firmware signing ensures the integrity and authenticity of upgrade packages—before applying any upgrade, the device verifies the signature and rejects the package if verification fails, preventing tampered or forged firmware from being installed through the upgrade channel.

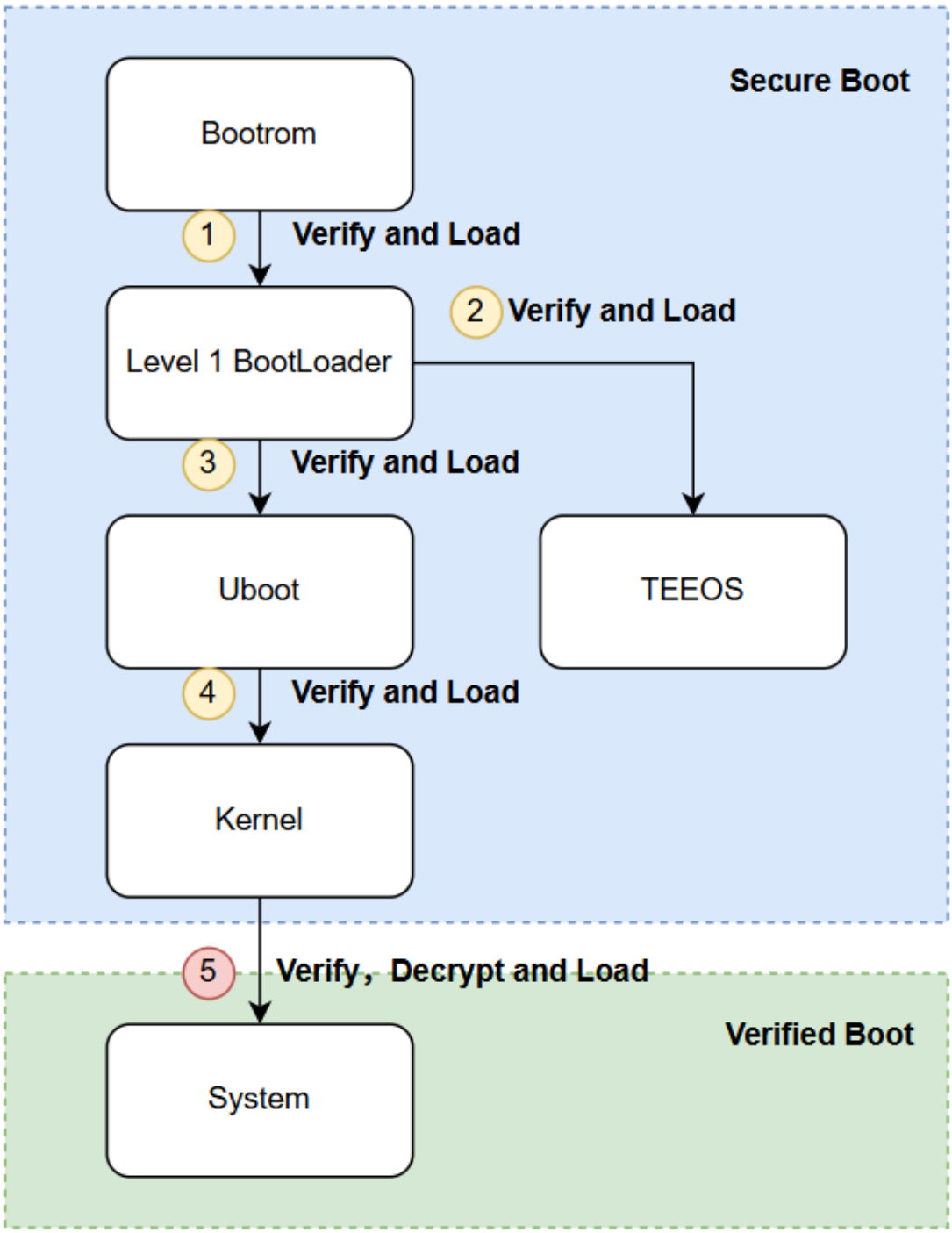

Figure 2: Secure Boot + Verified Boot + File System Encryption

In addition to these default protections, Fleet Hub provides two user-initiated security functions during the device's operational lifecycle. Log export is encrypted by default; factory reset can be performed at the user's discretion:

- **Encrypted Log Export:** Log export is an important tool for troubleshooting and technical support diagnostics. Exported logs are encrypted by default using AES-256-

CBC to protect their confidentiality. Log export is always user-initiated—Bambu Lab does not proactively collect or retrieve device logs. Diagnostic logs submitted to Bambu Lab through a support ticket are automatically deleted 14 days after the ticket is closed.

- **Factory Reset:** When Fleet Hub is decommissioned, transferred, or needs to be repurposed, factory reset permanently clears all user data from the device—including activation information, account credentials, system logs, model file cache, and all temporary data. The device restarts automatically into its unactivated initial state, ensuring no data residue remains after decommissioning.

4. Network and Communication Security

The combination of hardware trust roots and system-level hardening significantly raises the bar against physical attack vectors. However, network services and communications are Fleet Hub's core functionality—and therefore its most significant attack surface.

Fleet Hub was designed with network and communication security as a first-class architectural concern. As an enterprise device deployed within customer-controlled networks, particular attention was given to enterprise network compatibility and strict control over outbound traffic. Key measures are as follows:

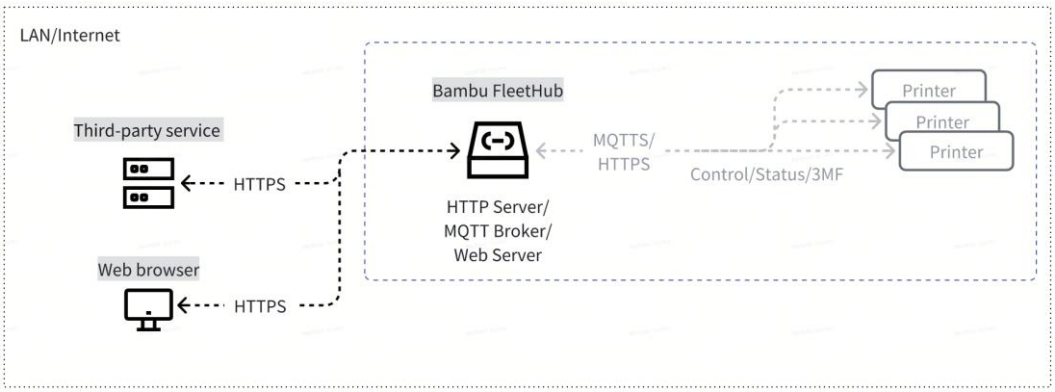

Figure 3: ***Communication Topology***

- **Minimized Attack Surface:** Only the ports necessary for operation are exposed. All other ports are closed by default, leaving attackers with minimal footholds.
- **End-to-End TLS/mTLS:** With the exception of the SSDP discovery service, all communication channels use TLS or mutual TLS (mTLS).

- **Enterprise Network Support:** Fleet Hub supports WPA2-Enterprise for connecting to enterprise wireless networks, covering EAP-TLS, PEAP (MSCHAPv2), and TTLS (MSCHAPv2/MSCHAP).
- **Data Stays on the LAN:** After activation, Fleet Hub does not proactively initiate any outbound data uploads or control connections to external networks. All user data and print operations remain within the local network.

Upon activation, Fleet Hub opens only the following communication ports. All other ports remain closed by default. Except for the SSDP service—which is used solely to broadcast the device's presence on the local network—all other channels use TLS or mTLS.

Port	Protocol	Encryption	Purpose
TCP/443	HTTPS	TLS	Web management interface, only used after setting up a web account
TCP/8888	HTTPS	mTLS (mutual)	Third-party service API / model file transfer
TCP/1883	MQTTs	mTLS (mutual)	Fleet Hub–printer control channel
UDP/1990, 1991, 2021, 2022	SSDP	None	Local network device discovery

Table 1: Fleet Hub Open Ports

5. Identity and Access Control

Fleet Hub's identity and access control layer combines certificate-based identity, account-based permissions, and access tokens. Certificates establish machine-level trust between devices and services; accounts define what operations may be performed; tokens control session validity and API call scope. Together, these three mechanisms form the access control baseline for Fleet Hub.

5.1 Certificate Infrastructure

Fleet Hub's communication endpoints use an X.509 end-entity certificate infrastructure covering three entity types: Fleet Hub devices, 3D printer devices, and

third-party services. Fleet Hub and printer certificates are injected at the production line and are unique per device; third-party services must register with Bambu Lab to obtain an access certificate. These certificates are the trust foundation for mTLS. With the exception of the Web management interface, all core communication channels use mTLS mutual authentication (minimum TLS 1.2), blocking unauthorized endpoints at the connection establishment stage.

Fleet Hub Activation and Certificate Binding

Fleet Hub must be activated before use. The activation process establishes and anchors a three-party trust relationship: Fleet Hub first verifies the third-party service's certificate and generates an Active Ticket; the third-party service submits the Ticket to Bambu Lab's cloud service in exchange for a signed Active License; Fleet Hub verifies the signature of the Active License and completes activation upon success. Once activated, the device identity, service identity, and authorization relationship enter a verifiable state, providing the trust prerequisite for subsequent API calls and device control. Critically, activation binds Fleet Hub to the specific third-party service certificate used during activation—even another certificate legitimately issued by Bambu Lab to a different service will be rejected.

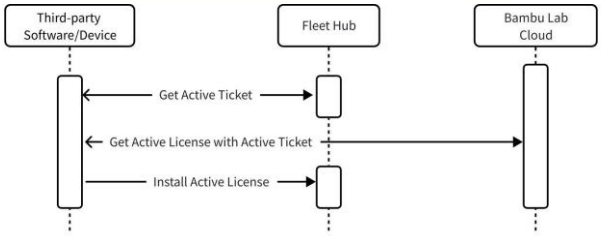

Figure 4: ***Device Activation Process***

5.2 Account System

If the certificate infrastructure answers the question "which machine is this?", the account system answers "what is this entity allowed to do?". Fleet Hub separates machine identity authentication from operational permission authentication, avoiding the risk of privilege sprawl that comes with relying on a single credential model. Two types of accounts are used in Fleet Hub: the Local API Account and the Web Management Account.

Local API Account

The Local API Account is created during activation and is the mandatory credential for all subsequent programmatic API calls. Only one Local API Account is supported per device. Password requirements: at least 8 characters, containing at least one digit, one uppercase letter, one lowercase letter, and one special character. The

account and its key are stored exclusively in Fleet Hub's internal secure storage and cannot be exported in plaintext. After logging in with the API Account, the system issues a JWT Token for subsequent requests; once the token expires, re-authentication is required, reducing the risk of long-term session abuse.

Important: If the password is lost, the only recovery option is a factory reset, which will erase all activation information and data. Please store credentials securely.

Web Management Account

The Web Client Account is an optional operations account that does not exist by default and can only be created by an already-authenticated API Account. Only one Web Client Account is supported per device. The web interface uses username and password authentication over a TLS-encrypted channel. A weak password check is performed at creation time to reject commonly used passwords. If no Web Client Account is created, the built-in web management interface cannot be accessed, reducing the exposure and attack surface of that entry point.

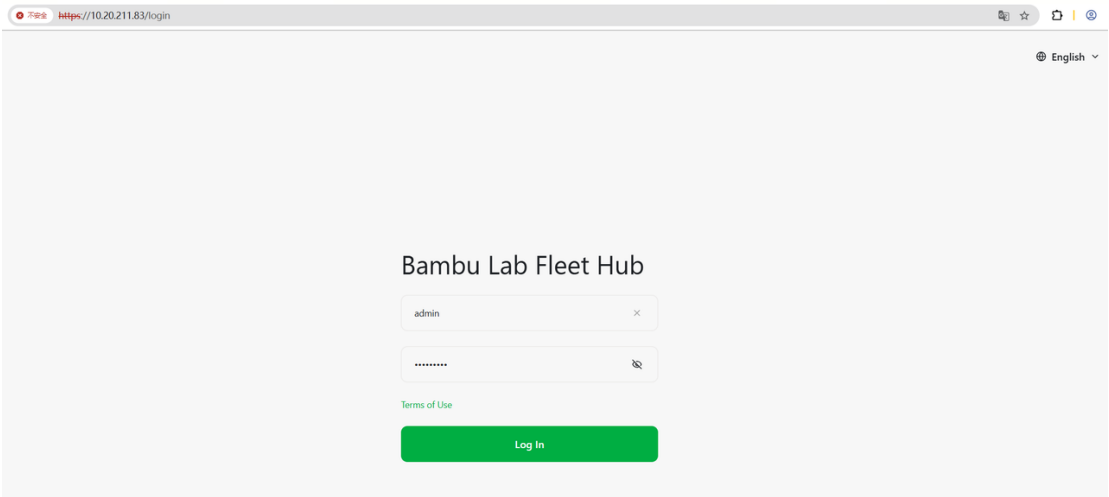

Figure 5: ***Web Client Management Interface***

Password Security Recommendations: Use a strong, unique password that is not reused across other systems. A minimum length of 12 characters is recommended. Avoid using the same password as the API Account. Rotate credentials immediately upon personnel changes or suspected compromise, and manage credentials using enterprise-grade credential management tools.

6. Model and Data Protection

The preceding chapters addressed "who can access Fleet Hub and how trust is established." This chapter addresses "whether data is secure during storage and transmission." In the course of executing print jobs, Fleet Hub handles the service provider's most critical business assets—model files entrusted by their clients, along with operational data and logs generated during printing. Fleet Hub implements targeted protections across model transmission, local storage, and data lifecycle management.

- **Encrypted Model Upload:** When a third-party service uploads model files to Fleet Hub, the transfer uses mTLS-encrypted HTTPS (TCP/8888), ensuring files cannot be intercepted or tampered with in transit.
- **Encrypted Model Download:** When a printer downloads a model file from Fleet Hub, the transfer also uses HTTPS. If the printer downloads from a third-party storage server directly (custom URL download), HTTPS is mandatory—plaintext HTTP is not supported. If the third-party storage uses a self-signed certificate, the root CA or intermediate certificate chain (PEM format) must be pre-injected into the printer via the Fleet Hub API before the download can proceed.
- **Data Stays on the LAN:** After activation, Fleet Hub does not upload any data to external servers. Model files are stored locally on Fleet Hub and are never transmitted to Bambu Lab's cloud or any other external service.

- **Local Storage:** Fleet Hub provides 40 GB of local storage for model file caching. When storage space is insufficient, the oldest files are automatically deleted to free space.
- **Model Encryption at Rest (Planned):** In the current version, model files are stored in plaintext on Fleet Hub's local storage. A future version is planned to introduce encrypted storage for model files at rest, preventing an attacker with physical access to the device from extracting plaintext model data. In the meantime, we recommend deploying Fleet Hub in a physically access-controlled environment.

In addition to model files, Fleet Hub caches camera snapshots from printers during print jobs for monitoring purposes. Snapshot data is stored locally on Fleet Hub only and is never transmitted to external networks. Snapshots can be permanently cleared by performing a factory reset.

Data Type	Storage Location	Retention Policy	After Factory Reset

Activation info and account credentials	Fleet Hub local storage	Valid for the device's operational lifetime	Cleared
Model file cache	Fleet Hub local storage	Oldest files deleted automatically when storage is insufficient	Cleared
Printer camera snapshots	Fleet Hub local storage	Only the latest snapshot from the most recent print job is cached; previous snapshots are overwritten	Cleared
System logs	Fleet Hub local storage	User-initiated export only; unexported logs never leave the device	Cleared
Diagnostic logs submitted to Bambu Lab	Bambu Lab support system	Auto-deleted 14 days after ticket closure	--

Table 2: Data Lifecycle

7. Security Compliance and Organizational Governance

Technical controls are the foundation of any security program, but security is not a one-time engineering effort. It requires continuous validation, process discipline, and external accountability. This chapter describes the organizational-level security and compliance mechanisms Bambu Lab has established for Fleet Hub.

Security Certifications: Bambu Lab has obtained the following international security and privacy certifications, covering product development, data handling, and operational processes. As a component of the Bambu Lab product ecosystem, Fleet Hub falls within the scope of these certifications:

- **ISO/IEC 27001**: The international information security management system

standard. This certification means Bambu Lab's development and operations processes are subject to annual third-party audits.

- **ISO/IEC 27701**: The international privacy information management system standard, covering how user data is collected, processed, and protected.
- **TRUSTe Enterprise Privacy**: An internationally recognized privacy and data governance framework certification, assessed by a third-party organization specializing in privacy protection.

Security Testing: Bambu Lab has established an internal security team that continuously validates the security of its products through multiple methods:

- **Internal Penetration Testing**: The internal security team conducts regular manual penetration tests against Bambu Lab products, simulating real-world attack scenarios to verify that defenses hold in practice.
- **External Penetration Testing**: Bambu Lab products undergo periodic independent security assessments by qualified third-party security firms, providing an objective evaluation of the security program's completeness.
- **AI-Assisted Code Auditing**: AI-powered tools are integrated into the development phase to perform automated security reviews of code, identifying potential vulnerability patterns and risk areas before they reach production.
- **AI-Assisted Automated Penetration Testing**: AI tools are used to conduct automated penetration tests against product network interfaces and APIs on an ongoing basis, validating the effectiveness of security boundaries.

Bug Bounty and Security Feedback: Bambu Lab welcomes security researchers, enterprise customers, and partners to report security issues related to Fleet Hub. Every submission is taken seriously and fed into our product improvement and release cycle.

- Bug Bounty Program: https://bambulab.com/en/bug-bounty-program
- Security Contact: security@bambulab.com