Bambu Lab
Security White Paper

2025.09

Catalog

01
Introduction

Bambu Lab is a company founded in 2020 and headquartered in Shenzhen, China, with a mission to revolutionize the desktop 3D printing industry through cutting-edge robotics. The company has R&D centers in Shenzhen and Shanghai, as well as an office in Austin, Texas.

Bambu Lab's products have achieved a significant leap forward in key performance areas. The company has introduced industrial-grade features, such as multi-color printing and support for high-performance engineering plastics, into consumer-level products. This empowers users to overcome limitations in color and material, elevating their creativity to a new level and helping them rediscover the pure joy of creation.

Even though our founding team had extensive experience in robotics, we initially lacked expertise in cybersecurity. The community was the first to raise concerns about security vulnerabilities in our early products, which served as a crucial wake-up call. It made us realize that product cybersecurity and user data privacy were our undeniable responsibilities.

For the past three years, we have made cybersecurity and user data privacy one of our top priorities. We've continuously invested in personnel, collaborated openly with industry security experts, research institutions, and partners, and taken ongoing actions to improve the security of our products.

This security whitepaper documents Bambu Lab's continuous investment and exploration in the fields of cybersecurity and data privacy over the past three years. We deeply understand and respect the importance our users place on cybersecurity and data privacy, viewing it as a cornerstone of our operations. We also sincerely thank the community for their invaluable feedback, which has pushed us to constantly learn and improve. In the future, Bambu Lab will continue to embrace an open and transparent approach, fostering public collaboration to build more robust security protections and safeguard every user's creative journey.

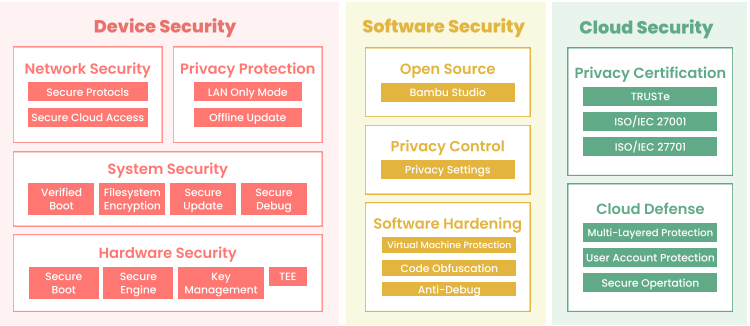

Figure 1: Security Defense System

This whitepaper will delve into the following structure to elaborate on the security architecture, technical principles, functional design, and privacy protection measures for Bambu Lab's 3D printers and related software and cloud services. We hope this document will promote greater clarity and transparency in the architecture and implementation of these measures.

Device Security
A combination of software and hardware to build device security, network security, and data security features.

Software Security
Protecting software through virtual machine protection and runtime defense mechanisms to reduce the risk of attacks on user-side software.

Cloud Service Security
Adopting a multi-layered cloud defense mechanism to protect cloud security through security management and periodic penetration testing.

Privacy Compliance
We firmly believe that user privacy data is a core user value. Our security and privacy organizational processes are internationally certified.

Open-Source Initiatives
We have learned a great deal from the community and are eager to give back. We respect the open-source community and open-source agreements and strictly adhere to our open-source plan.

Bug Bounty Program
Seeking public collaboration with security experts, research institutions, and industry partners to collectively enhance our security protection capabilities.

If you would like to discuss any security-related issues with us, please contact us at security@bambulab.com. We highly value every piece of user feedback and will take all necessary measures to improve the security of our products.

02
Device Security

In the Bambu Lab product ecosystem, 3D printer product security is paramount, with device security being the core component. For one, 3D printers inevitably process users' design models and parameters during operation. Unauthorized access or cyberattacks could easily lead to the leakage of users' intellectual property and business secrets. Additionally, since 3D printers are often used in homes, malicious control could trigger dangerous printing behaviors, potentially leading to serious safety hazards like fires.

We firmly believe that as the 3D printing market matures, user demands for device security will continue to rise. Superior product security isn't just a key competitive advantage for future 3D printers; it is also crucial for Bambu Lab to earn user trust and set an industry benchmark.

2.1 Hardware Security

Hardware security infrastructure is the foundation of device security. Without its support, software-level protections can be easily compromised, and cryptographic keys are difficult to protect effectively, making it impossible to ensure user network and data privacy.

Bambu Lab hardens its systems by using technologies such as secure boot, secure key management, a secure cryptographic engine, and a trusted execution environment. These work in close combination with the upper-layer software to maximize the protection of user data privacy.

2.1.1 Hardware Trust Environment

Secure Engine And Key Management
All Bambu Lab 3D printers are equipped with a hardware-based security engine that can perform cryptographic operations using keys stored in a One-Time Programmable (OTP) area. Once written, the key will be placed under controlled access. This design effectively prevents key leakage.

The security engines in the X1 series and H2 series support mainstream symmetric and asymmetric algorithms, such as AES, SHA, and RSA, as well as hashing algorithms. The P1 series and A1 series support common algorithms like AES-XTS, HMAC, and RSA signatures.

Additionally, Bambu Lab follows NIST recommendations (https://www.keylength.com/en/compare) for choosing compliant algorithms, key strengths, and usage as shown in the table below.

Algorithm	Strength (bits)	NIST Recommendation	Usage
AES	128	2030	Encryption
RSA	2048	2030	Signature
ECC	256	2030	Authentication
ECDSA	256	2030	Signature
SHA	256	2030	Hash

Table 1: Recommended Cryptographic Algorithm Strengths as per NIST Guidelines

Trust Execution Environment
The X1 series and H2 series Bambu Lab printers use ARM® Cortex®-A series processors, which support ARM® TrustZone® technology. This is a Trusted Execution Environment (TEE) technology that uses hardware to divide the processor into a secure world and a normal world. In Bambu Lab's implementation, critical security features such as key management, secure storage, and firmware decryption and verification are all executed in the secure world. The purpose of this TEE is to ensure the integrity of these security functions and the confidentiality of the keys.

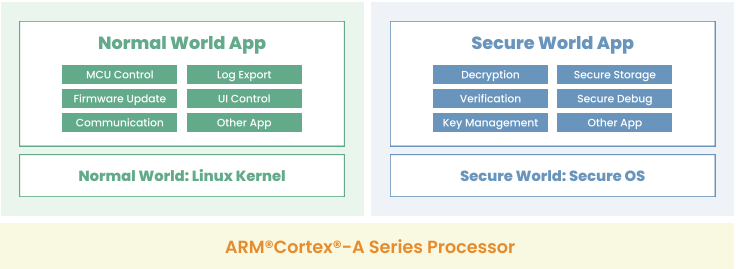

Figure 2: Isolation of Normal World and Secure World

Secure Storage Based On RPMB
Bambu Lab's X1 series and H2 series printers support Replay Protected Memory Block (RPMB). RPMB is a secure area in the device's storage that uses signature and replay protection mechanisms to ensure data can only be accessed by the TEE and to prevent unauthorized access. Bambu Lab uses RPMB to implement secure storage. Data written to RPMB is encrypted and can only be modified via the TEE. This allows critical data and flags to be securely recorded, preventing attackers from maliciously tampering with key data and compromising user privacy and data security.

Secure Storage Based On Flash Encryption
The P1 series and A1 series Bambu Lab printers implement secure storage using flash-based AES-XTS-256 transparent encryption and decryption. The key is stored in Efuse, and it can only be read and used by the hardware security engine. This encrypted flash partition prevents attackers from obtaining plain-text data from the flash through physical attacks, thus protecting user privacy and data security.

Device Attestation
To ensure the authenticity of each 3D printer, Bambu Lab pre-installs a unique device certificate on every machine. The public keys for these certificates are centrally stored on Bambu Lab's servers, while the private keys are securely stored on the device itself. In scenarios requiring device authentication, the printer can send a verification request to Bambu Lab's servers to confirm its authenticity.

2.1.2 Secure Boot

Secure Boot
All Bambu Lab printer models support Secure Boot. The principle of Secure Boot is that when the device starts up, the processor executes the BootROM code stored in the on-chip read-only memory. This code is fused into the chip during manufacturing and cannot be tampered with.

The BootROM verifies the second-stage bootloader stored in the flash memory. After successful verification, the firmware is loaded. Every step of this boot process undergoes signature verification to ensure the integrity of each piece of firmware.

Verified Boot
The X and H series Bambu Lab printers also support Verified Boot. While Secure Boot primarily verifies the integrity of the boot firmware, it does not verify whether the file system has been tampered with. Verified Boot technology, on the other hand, can check if the System partition's file system has been modified during startup. The combination of Secure Boot and Verified Boot effectively defends against the installation of malicious software or rootkits on the printer.

File System Encryption
The X1 series and H2 series Bambu Lab printers also support file system encryption. This feature is primarily used to protect the confidentiality of the System partition, making it significantly more difficult for attackers to perform reverse engineering. By raising this barrier, the overall security of the system is strengthened, which in turn helps protect user data and privacy.

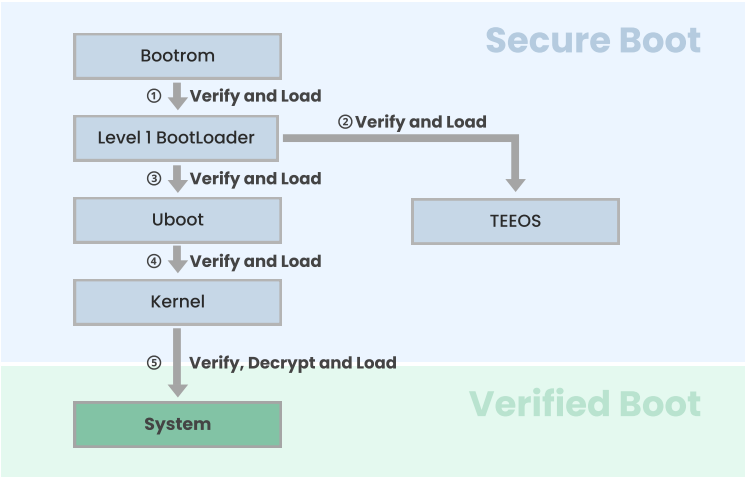

Figure 3: X and H Series Secure Boot + Verified Boot

2.2 System Security

If hardware security is the foundation of a system, then system security is the crucial barrier built upon that solid foundation. It encompasses various aspects, including the operating system and applications, aiming to use diverse software mechanisms to prevent security threats such as malware intrusion, unauthorized access, and data leakage.

2.2.1 Kernel Security

Mandatory Access Control
Bambu Lab's high-end printer models support Mandatory Access Control (MAC) . Mandatory Access Control (MAC) sets fine-grained security policies for applications by pre-defining and enforcing access rules. This allows for precise control over the system resources each application can access, including the file system, network, devices, and other inter-process communication interfaces.

By using Mandatory Access Control (MAC) measures, even if an application has a security vulnerability that is exploited, the damage it can cause is strictly limited to a predefined scope. MAC enhances the overall defensive depth of the device, thereby safeguarding user privacy and operational safety. This feature is currently supported on H2C, and will be extended to all X series and H2 series products.

KASLR
Bambu Lab's high-end models support the Kernel Address Space Layout Randomization (KASLR) security feature. KASLR randomizes the base address where the kernel is loaded each time the system boots. This makes it difficult for attackers to predict the kernel's memory layout, which significantly increases the difficulty of code reuse attacks. As code reuse attacks are a common method for modern kernel exploits, using KASLR effectively enhances kernel security, thus protecting user data privacy. This feature is currently supported on H2C, and will be extended to all X series and H2 series products.

2.2.2 Secure Update

All Bambu Lab 3D printers support a secure firmware update feature, which is typically used for releasing new features, bug fixes, or security patches.

After being developed and tested by Bambu Lab, the firmware is encrypted and signed before being uploaded to our firmware servers. Once verified, the firmware is officially released. Users can then update their printers either through the App or by downloading the firmware to to an SD card or USB Drive for offline update.

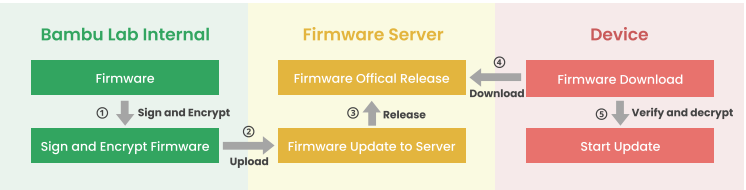

Figure 4: Secure Firmware Update

The firmware signing keys are strictly protected within Bambu Lab. The public key's hash is stored in the Efuse on the device, ensuring that even if the device is compromised, attackers cannot tamper with the public key or obtain the private key.

On Bambu Lab's high-end models, firmware decryption and signature verification are performed within the Trusted Execution Environment (TEE), leveraging the hardware infrastructure to further increase the difficulty for attackers.

Firmware encryption and firmware signing ensure the confidentiality and integrity of the firmware.

- Encryption makes reverse engineering more difficult, increasing the barrier for attackers.
- Signing prevents malicious or tampered firmware from being installed on a user's device, thereby protecting user data and privacy.

2.2.3 Debug Channel Disabled

At the factory, debugging methods like JTAG and serial ports are disabled on all Bambu Lab products. This prevents attackers from using these interfaces to extract firmware or alter its operating logic. This enhances firmware security, effectively stopping printer intrusions and user data leaks.

2.3 Network Security

One of the core features of Bambu Lab's 3D printers is their ability to connect to our cloud services. This "cloud connectivity" significantly expands the user experience, enabling key functions like sending models and print tasks, remote monitoring, receiving firmware updates, and accessing the model library. This brings users unprecedented convenience and efficiency.

However, while network connectivity brings convenience, it also introduces potential security risks. If a device is exposed to an insecure network or has vulnerabilities in its network defenses, it could face threats like unauthorized access, data leaks, malicious control, or even service interruptions. Therefore, ensuring the network security of the 3D printer device itself is of utmost importance.

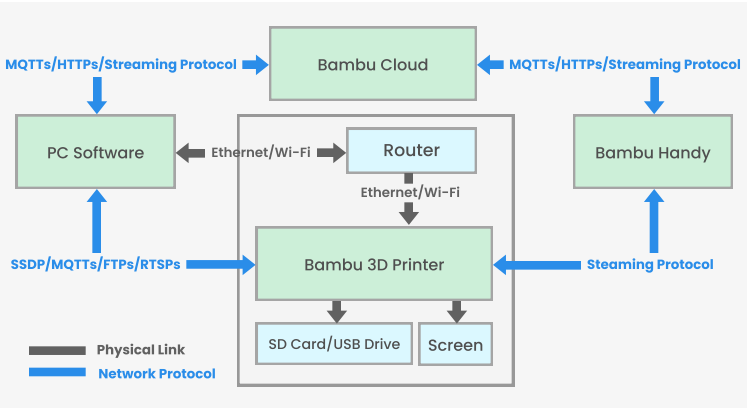

Figure 5: Bambu Lab 3D Printer Network Topology

2.3.1 Secure Network Protocols

Implementing secure network protocols can reduce the risk of data leakage and tampering when a user's device connects to the network. Bambu Lab's 3D printers use secure communication protocols by default, including HTTPs, RTSPs, MQTTs, FTPs, and DTLS protocol. Communication data is encrypted and signed, and the identity of the other party is verified, effectively mitigating the risk of user data being compromised.

Bambu Lab 3D printers support both wired and Wi-Fi connections. For Wi-Fi, they use security protocols including WPA/WPA2-PSK. WPA2 authenticates each connection and provides 128-bit AES encryption to help ensure the confidentiality of data sent over the air. This common encryption protocol ensures that user data is always protected when sent and received over a Wi-Fi network.

Bambu Lab's enterprise models (X1E and H2D Pro) also support WPA2-Enterprise, which offers enhanced security. By implementing individual user authentication, advanced authentication methods, and encryption, WPA2-Enterprise helps ensure the confidentiality, integrity, and authenticity of wireless communication in an enterprise environment.

The Bambu Lab P1 series supports Bluetooth Low Energy (BLE) for printer network configuration and binding via the Handy app. It uses AES-CMAC and P-256 elliptic curves, along with the AES-CCM protocol, to ensure secure pairing.

Bambu Lab printers can also operate in LAN Only Mode, allowing them to function without cloud communication. In this mode, control of the printer is handled through a locally deployed control protocol and an internal MQTTs server. File transfers are conducted using FTPS for secure file uploads and downloads.

2.3.2 Secure Cloud Access

To provide remote control functionality for its printers, Bambu Lab utilizes IoT services that include features such as device login, device information synchronization, firmware/software updates, user-device binding, remote printing, slicing parameter management, cloud slicing, and fault detection.

Device Login
Each device is assigned a unique, built-in ID of at least 120 bits and password, both randomly generated at the factory. When a device connects to our IoT services, a mutual authentication process takes place between the cloud and the device.

The device verifies the cloud service's identity, and the cloud service verifies the device's identity. The device's identity relies on the public-private key pair embedded during manufacturing. Only after this mutual authentication is successful can the device connect to the IoT service.

Following mutual authentication, the cloud performs a further check to verify the device's authenticity. This prevents a scenario where a large number of counterfeit devices could be created on the cloud if a public-private key pair were to be accidentally leaked.

Device Binding
Here are three ways a printer can be connected to a user account:

1. **Scanning a QR Code:** A QR code is displayed on the printer and is valid for 5 minutes.
2. **Using SSDP:** The printer can be connected over a local network using SSDP information.
3. **Via Bluetooth:** The connection can be established through a Bluetooth connection.

All three device binding methods will be carried out through secure binding protocols.

Models Upload Security
G-code files can be sent to the printer via a local network connection or, with a stable internet connection, through our cloud service. When a file is sent via our cloud service, the G-code is transmitted over a secure HTTPS channel to a temporary, private storage location. The uploaded file includes an expiration date and a corresponding authentication signature, and it can only be used for the upload, maximizing data security.

Once the file is uploaded to the cloud, the printer receives the print file address from the MQTT print command, downloads the file locally, and parses it before starting the printing process. Users can configure their privacy settings in the Bambu Handy App:

- If stealth mode is enabled, the temporary G-code file stored in the cloud will be automatically deleted after 3 days.
- If stealth mode is not enabled, the temporary file will be automatically deleted after 90 days, allowing the user to initiate a reprint from the cloud within that timeframe.

Video Stream Service Security
Cloud connectivity acts as a secure intermediary for video streaming services, authenticating requests and providing streams to the client. Both the video streams and file transfers are protected by TLS/DTLS encryption, ensuring a secure and authorized link. Once the handshake is completed to authorize the stream, the connection is established directly between the Handy App / Studio and the printer, bypassing our servers entirely, thereby ensuring end-to-end privacy and minimal latency.

2.3.3 Accessory Security Verification

3D printers rely on a wide variety of accessories, and Bambu Lab 3D printers are primarily designed to work with original Bambu accessories. Depending on their function, certain accessories may affect print quality, damage the printer, or even pose risks to user safety and property. For these critical components, we implement a security certification process to prevent unauthorized or potentially hazardous accessories from being used.

Each certified accessory is equipped with a unique public-private key pair. When connected to the 3D printer, the printer performs a challenge-response authentication to verify the authenticity of the accessory, ensuring that critical components are legitimate rather than unauthorized. This mechanism effectively reduces potential security risks.

2.3.4 Authorization Control

Being exposed to a network environment, 3D printers face the risk of remote attacks. Our continuous cloud service operations have also detected a massive volume of anomalous requests daily from non-official clients, which seriously threatens our service availability.

Therefore, we have designed an Authorization Control feature. The idea behind this is to add a protection mechanism for the connection and control of Bambu Lab 3D printers through authorization and authentication. This ensures that only authorized access and operations are permitted, while all unauthorized attempts are denied.

Principle of Authorization Control
The authorization control feature works by authenticating critical commands sent to the printer. Before executing a command, the printer verifies that its signature is correct.

Under normal operation, Bambu Studio communicates with the printer through a network plugin. When authorization control is enabled, this plugin authenticates the software that calls it (using the software's signature—this is currently supported on Windows and macOS, but not yet on Linux). Only software that has been authenticated can initiate critical control commands.

This is because the network plugin has a built-in private key. Commands from unauthenticated software will not be signed, and the 3D printer will not execute any command for which the signature verification fails. This ensures that only authorized software can control the printer. While this built-in private key is not hardware-protected, a combination of multiple software hardening methods significantly increases the barrier for attackers.

The Authorization Control feature restricts third-party software from directly calling dangerous interfaces without control, but this also impacts Non-malicious third-party software that needs to access Bambu Lab printers.

To address this, we developed Bambu Connect. This software provides a streamlined user interface with integrated security protocols, simplifying third-party software integration. With Bambu Connect, you can safely initiate printing tasks. It also has a built-in private key and uses the same software hardening methods as the network plugin, which helps raise the barrier for attackers.

LAN Only - Developer Mode

After the release of Authorization Control and Bambu Connect, we received widespread feedback, with many print farm owners expressing concerns about reliable, uninterrupted access to their 3D printers. We understand the risks these businesses face, and although the Authorization Control feature was still in its beta phase, it could still affect devices or third-party software used in print farms.

Consequently, we decided to add a new option for LAN Only Mode: Developer Mode. This feature is designed to give advanced users greater control and flexibility.

With Developer Mode, the printer's MQTTs will not be governed by the Authorization Control feature, allowing third-party software to function normally. Users also have the option to either not upgrade their firmware or to downgrade to a version released before Authorization Control was enabled, which will also allow them to continue using third-party software.

You can find more information about using Developer Mode by following this link: https://wiki.bambulab.com/en/knowledge-sharing/enable-developer-mode

Contact Email

If you have any feedback regarding the Authorization Control feature, or if you are a third-party software developer interested in a partnership, please contact us at devpartner@bambulab.com.

2.4 Privacy Protection Feature

We understand the importance our users place on privacy and data security. We continuously listen to their needs and optimize our products accordingly. While user concerns can never be completely eliminated, we choose to listen and respect them, turning these concerns into concrete actions. Our goal is to strike a balance between convenience and privacy protection.

Currently, our devices offer users the following privacy protection features:

2.4.1 LAN Only Mode

When a 3D printer is connected to network, it offers convenience but also raises privacy and data security concerns for users. After listening to user feedback, we developed LAN Only Mode for those with such concerns.

In LAN Only Mode, the 3D printer will not initiate any external connections, and the Bambu Handy app will not be functional. All communication between the client software and the printer takes place within the local network. Communication protocols in this mode still use secure methods (SSDP, MQTTs, FTPs, RTSPs, etc.), preventing potential attackers on the local network from listening in on or tampering with data.

In LAN Only Mode, client software connects to the device by entering the device's PIN code. This binding process also happens exclusively on the local network, without needing to connect to a server.

This device binding feature provides access control for the printer within the local network, preventing potential malicious devices on the same network from directly controlling the printer and creating security risks.

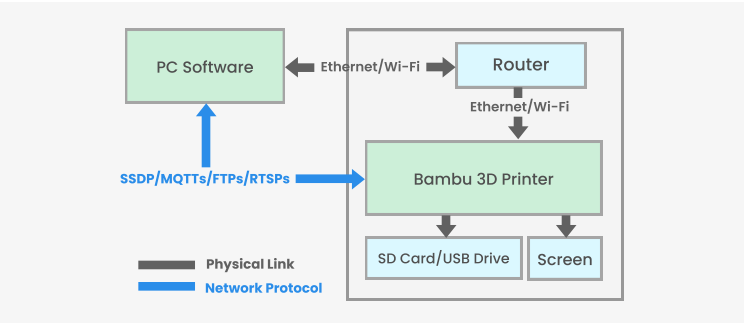

Figure 6: LAN Only Mode Network Connection

For instructions on how to enable LAN Only Mode, please refer to the following link: https://wiki.bambulab.com/en/knowledge-sharing/enable-lan-mode

For those who still have privacy concerns with LAN-only Mode, Bambu 3D printers can be used entirely offline. Simply disconnect from the network and use an SD card or USB Drive to print your models.

2.4.2 Network Switch

The X1E and H2D Pro models support a network switch feature. On the X1E, the network switch can be used to disable both wired and wireless connections, thereby preventing any potential data transmission. On the H2D Pro, this feature has been further enhanced: the network switch can completely power off the wireless module to ensure it is fully disabled, while wired connectivity can be cut off simply by disconnecting the cable.

With the network switch functionality, enterprise models can operate securely within user environments, effectively addressing the stringent privacy and security requirements of enterprise customers.

2.4.3 Offline Update

While LAN Only Mode prevents data from connecting to cloud services, it also restricts the availability of features that require an internet connection, such as firmware updates. Users in this mode cannot update their firmware, and connecting to the network to do so would compromise their original privacy and data security settings.

After listening to user feedback, we decided to offer an offline update feature. This allows users to update their firmware using an SD card while remaining in LAN Only Mode.

Figure 7: Offline Update

The offline update feature allows users with privacy and data security concerns to use the latest firmware features while maintaining their original privacy and data security settings.

2.4.4 Log Export Encryption

The log export encryption feature was initially designed to defend against network attacks and protect user privacy.

On one hand, it prevents unauthorized individuals from directly accessing a user's plain-text log information, thereby protecting private data. On the other hand, exporting certain information in logs in plain text could pose cybersecurity risks. For example, address information in kernel logs could be used by an attacker to bypass kernel security protections like KASLR, significantly increasing the risk of code reuse attacks.

After these events, we decided to add more transparency to the log export process, striking a balance between protecting network security, safeguarding user privacy, and providing user transparency.

While logs are still encrypted with the AES algorithm during export, we have added explanations and options that allow users to decide what data to send us based on their specific situation.

Bambu Lab's high-end models support log export via SD card. The X1 series supports AES-128 log encryption, while the H2 series supports AES-256 log encryption. These high-end models support the export of three main data types: system logs, sensor data, and G-code. Users can choose whether to export sensor data and G-code. Sensor data is helpful for diagnosing issues related to LiDAR and spaghetti detection, while G-code is useful for assessing print quality problems. Users can select which data to export based on their specific situation.

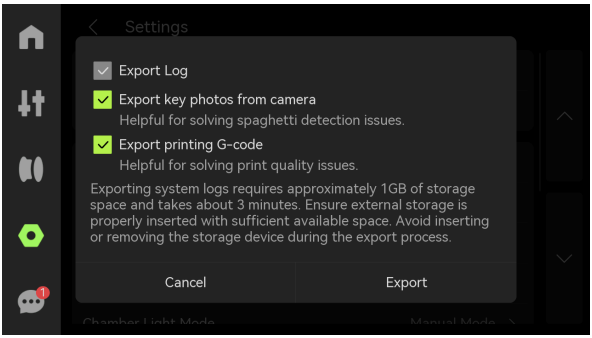

Figure 8：Log Export Options on H2D

On the Bambu Lab P1 series and A1 series printers, logs are encrypted by default using the AES-128 algorithm and stored on the SD card. Users can submit the relevant logs as needed.

The logs generally serve the following purposes:

- **logger:** Provides concise printing process logs. This is the primary log to consult for all troubleshooting.
- **recorder:** Contains critical logs for diagnosing issues such as abnormal leveling/calibration, print quality problems, print stoppages caused by sensor errors, failed prints, and other unexpected interruptions during printing.
- **corelogger:** Records system status information during exceptions and is used to diagnose issues where a print stops unexpectedly.

On all Bambu Lab printers, the log export feature is initiated entirely by the user. Bambu Lab cannot access a user's log data unless it is actively uploaded by the user. Any logs that are uploaded are automatically deleted 14 days after the support ticket has been resolved.

For more details on log encryption, export, and upload, please refer to the following link: https://wiki.bambulab.com/en/X1/troubleshooting/how-to-upload-log

2.4.5 **Factory Reset**

Bambu Lab 3D printers support a factory reset feature, which, when performed, resets a user's configuration data.

- For the Bambu Lab X1 series and H2 series, log data is stored internally on the device, and a factory reset will also clear this log data.
- For the Bambu Lab P1 series and A1 series, log data is stored on the SD card by default. Users can clear this log data by formatting the SD card.

Figure 9：Format SD Card On P Series

2.4.6 **User Experience Improvement Plan**

This program is designed to continuously optimize and enhance the product experience. The data collected primarily includes anonymized information on device status and usage, which is used to analyze and improve the product.

Users can turn the User Experience Program on or off on the device by navigating to Settings > Device & SN > User Experience Program.

The data is encrypted and uploaded through a secure communication channel, ensuring it cannot be accessed by third parties.

03
Software Security

Within the Bambu Lab ecosystem, software serves as the essential bridge that connects devices, data, and workflows. Bambu Studio and Bambu Suite provide powerful tools for slicing and editing models. Bambu Network Plugins and Bambu Connect ensure seamless device interconnectivity. The intuitive Bambu Handy app offers convenient mobile control, while Bambu Farm enables streamlined management of large printer clusters. Together, these software solutions handle everything from printer connections and cloud access to model processing and centralized farm control, forming the foundation of a smooth and efficient 3D printing experience. The seamless operation of this software is essential for everything from connecting printers and accessing cloud services to processing model data and centralizing control of farm equipment. They are the key cornerstones for building a smooth and efficient 3D printing experience.

This software runs on a user's PC or mobile phone, and its security directly impacts the safety of the user's device, private data, and the entire 3D printing ecosystem. If the software contains security vulnerabilities—such as code defects, improper configurations, or a lack of necessary security protection—it could become an entry point for hackers. Maliciously repackaged software could also be implanted with Trojans, leading to the theft of user design files, malicious control of printers, personal information leaks, and even risks to the security of the user's network environment.

Therefore, comprehensive security hardening and signing of this software are critically important. Only when the security and integrity of the software are guaranteed can we ensure the stable and reliable operation of Bambu Lab's products and services, thereby protecting user assets and privacy.

However, we are also keenly aware that no software can ever be 100% secure, especially when it operates in an insecure environment. A well-trained and persistent attacker will, given enough time, eventually succeed. This is a dynamic attack and defense game. Despite this reality, we are firmly committed to adopting multi-layered security hardening techniques and strict software integrity protection mechanisms to significantly raise the entry barrier and cost for potential attackers. we are continuously working on improving and updating the software to keep up with new security threats that might come up. And that it is important to always update the devices and the software to the latest version for the highest security

3.1 Software Hardening

The purpose of software hardening is to prevent software from being reverse-engineered or repackaged with malicious code, thereby raising the barrier for attackers. Although Bambu Lab's software operates on various platforms (Windows, Linux, macOS, iOS, and Android), it consistently employs the following software hardening techniques:

3.1.1 Application And PC Software Signature

Bambu Lab's Bambu Handy App is available on the App Store for iOS users to download. Being listed on the App Store means the application has successfully passed Apple's rigorous security review process. When you install the app, the iOS system verifies its signature to ensure it has not been maliciously altered by a third party.

The Bambu Handy App for Android also undergoes a strict signing process and is available on the Google Play Store. Similar to the iOS platform, listing on Google Play requires passing its stringent security checks. Your Android phone will verify this signature during installation to confirm the software's integrity. Remember to only use the store version and the file downloaded from Bambu Lab website to avoid compromised installation apps.

Furthermore, Bambu Lab's PC software (Bambu Studio, Bambu Suite, Bambu Studio network plugin, and Bambu Connect) is digitally signed for both Windows and macOS versions. When you run these applications, your operating system will clearly indicate whether the software has been officially signed and released by Bambu Lab, effectively warning you against potential counterfeit or malicious programs.

On both Windows and macOS platforms, the Bambu Studio network plugin takes an extra security step by verifying the application signature of the software that is calling it. This prevents unauthorized programs from using the plugin's library to communicate directly with the printer.

3.1.2 Virtual Machine Protection

Virtual machine protection is a relatively mature technique used in the field of software anti-decompilation. Its core principle is to cleverly convert the native machine code of an executable program into a new, custom set of bytecode or instructions. These instructions do not execute directly on the underlying hardware; instead, they run within a carefully designed, software-implemented virtual machine environment.

The semantics of the native machine code are mapped to this new, unfamiliar set of virtual machine instructions. To understand and restore the program's true logic, an attacker not only needs standard disassembly and reverse engineering skills but also faces the more formidable challenge of first having to completely reverse-engineer the entire virtual machine's architecture, instruction set, and execution flow.

While virtual machine protection is not absolutely unbreakable, it significantly increases the complexity and time cost of reverse engineering, thereby greatly raising the barrier to attack.

Virtual machine protection is consistently used across Bambu Lab's apps and PC software to safeguard critical assets. These assets include core credentials like authentication tokens for cloud connections and message signing keys for printer communication.

We are well aware that even assets protected by virtual machines are not 100% secure against experienced attackers. Therefore, our overall security strategy doesn't solely depend on the absolute non-disclosure of this sensitive information. Instead, we use virtual machine protection as a key component to significantly raise the attack barrier, which in turn reduces the risk of being compromised.

3.1.3 Code Obfuscation

Code obfuscation is another common industry practice for combating decompilation. Its core idea is to use various transformation techniques to make a program's source or intermediate code difficult to understand and analyze, all while keeping its functionality intact. Compared to virtual machine protection, code obfuscation is less robust but also has a smaller system overhead.

Bambu Lab's apps and PC software consistently use code obfuscation techniques. While virtual machine protection is typically used to safeguard core assets and critical logic, code obfuscation is generally applied to non-core assets and non-critical logic. Although code obfuscation can't completely prevent a professional hacker's reverse engineering, it can still raise the attack barrier to some extent and reduce security risks.

3.1.4 Anti-Debug

Anti-debugging techniques are primarily used to prevent dynamic debugging of software. While virtual machine protection and code obfuscation are effective against static analysis, skilled attackers often combine dynamic and static analysis to successfully complete an attack. Anti-debugging techniques are specifically designed to address these dynamic debugging scenarios.

Bambu Lab's apps and PC software consistently use these techniques. Although anti-debugging alone cannot completely prevent a professional hacker's reverse-engineering efforts, it can still raise the barrier for dynamic debugging, which helps to reduce security risks.

3.1.5 Key Resource Encryption

Critical resource encryption is a method of protecting an application's key resources by encrypting them. Building upon the other security measures mentioned, this technique uses standard algorithms to encrypt critical resource files that may be used or loaded at runtime. These files are then decrypted only when needed, which helps to protect the resources and reduce the risk of them being leaked.

3.2 Software Privacy Protection

Our software and applications run on users' PCs and mobile phones, which means they interact with the users' device and data. Because of this, we are very cautious about the user permissions we request, ensuring that user privacy is fully protected.

3.2.1 Bambu Handy Privacy Permissions

The Bambu Handy application is designed under the principle of least privilege, requesting only the essential permissions required for its core functions. Users have the ability to manage and revoke certain permissions individually through their device settings. The purposes for which these permissions are requested are detailed below:

- **STORAGE:** Utilized for uploading or updating user account avatars and for commenting with image, video, or text content.
- **CAMERA:** Enables functions such as setting or updating avatars, photo album management, image saving, video recording, and barcode scanning.
- **LOCATION:** Specifically used for the network configuration of smart devices.
- **NOTIFICATION:** Facilitates the push of application-related messages.
- **INTERNET:** Provides network connectivity for device configuration and other online features.
- **BLUETOOTH:** Exclusively used for the network configuration of Bluetooth-enabled devices

3.2.2 Bambu Handy Privacy Settings

The Bambu Handy app provides users with a Privacy Settings feature, which can be configured by navigating to My -> Settings -> Privacy Settings.

Stealth Printing Settings
The Bambu Handy app supports Stealth Printing settings. When enabled, your print files will not be saved on the Bambu Cloud server. You can choose from the following three options based on your privacy preferences:

- **Disable Stealth Printing:** You can initiate prints directly from your print history.
- **Enable (with history):** Creates a history record, but your print files are not saved on the Bambu Cloud server.
- **Enable (no history):** Neither creates a history record nor saves your print files on the Bambu Cloud server.

Browse History Settings
The Bambu Handy app also supports Browse History settings, with two main options:

- **Enable Browse History:** Saves models you have viewed in the past 7 days, making it easy to find them again.
- **Disable Browse History:** When turned off, your Browse history is not recorded, so you will not be able to easily find models you have viewed.

3.2.3 Bambu Studio Experience Improvement Plan

The User Experience Improvement Program in Bambu Studio is designed to continuously optimize and enhance the user experience. The data collected primarily includes information on device status and usage, which is used to analyze and improve the product.

This data is encrypted and uploaded through a secure communication channel, ensuring it cannot be accessed by third parties. Users can freely opt-in or withdraw their authorization at any time by navigating to Preferences > User Experience in Bambu Studio.

04
Cloud Security

In the Bambu Lab product ecosystem, our cloud service is the crucial link connecting users with their devices, software, and the platform. By leveraging the cloud, users can effortlessly select models, initiate prints with ease, and remotely monitor and manage printing progress. While cloud services greatly enrich the use cases and value of 3D printing, they also present a higher challenge for data security and privacy protection.

Unlike a single device or local software, a cloud service must handle the centralized storage and processing of a massive amount of user data. This includes not only user design models, printing parameters, and usage records, but potentially also sensitive business information and personal data. Any unauthorized access, data leakage, or service interruption could have immeasurable consequences for a user's intellectual property, business continuity, and even personal safety.

4.1 Multi-Layered Security Protection

To ensure the security of its cloud services (including Bambu Cloud Service, MakerWorld, etc.), Bambu Lab has implemented a multi-layered security protection mechanism. As shown in the figure below, before a network request reaches the backend service, it passes through protection mechanisms such as a CDN, DDoS protection, and a Web Application Firewall (WAF).

Figure 10：Multi-Layered Security Protection

Bambu Lab's cloud services use secure communication protocols, including HTTPs，MQTTs and RTSPs, to ensure that the communication process cannot be eavesdropped on by third parties.

For the infrastructure used by our cloud services, Bambu Lab hosts data for overseas users on Amazon AWS (in the United States) and for Chinese users on Alibaba Cloud (in China). Both AWS and Alibaba Cloud have obtained certifications such as ISO 27001/27017/27018/27701 and SOC2. Additionally, Bambu Lab itself was certified with ISO/IEC 27001 and ISO/IEC 27701 on April 11, 2025.

When it comes to global security and acceleration, Bambu Lab utilizes the services of Cloudflare. As an independent edge network security provider, Cloudflare builds a secure, front-line defense layer between users and the Bambu Lab cloud platform across hundreds of data centers worldwide. This not only enhances the speed and stability of cross-regional access but also provides an efficient Web Application Firewall (WAF) and DDoS attack protection. In mainland China, Bambu Lab leverages Alibaba Cloud's WAF and DDoS protection alongside Cloudflare's global edge network.

The operation and maintenance of our cloud services are handled by Bambu Lab's professional operations team. We follow the best practices for resource management and security configuration recommended by both Amazon AWS and Alibaba Cloud, and we adhere to the Need-to-Know and Principle of Least Privilege policies. All permissions and operations performed on the server side are restricted by strict Standard Operating Procedures (SOPs) and are subject to control and audit mechanisms.

4.2 Bambu Account

Bambu account is used to identify Bambu Lab users, allowing them to access our products and services. We place great importance on the security and protection of user data. To safeguard user accounts, Bambu Lab has implemented a variety of login protection measures to ensure the security of your account data.

4.2.1 Login Methods

Bambu accounts support two login methods: username and password login, and third-party account login.

Login with Username and Password
In Mainland China, users can log in with a phone number and verification code, or with a phone number and password. In other regions, users can log in with an email and password. Users can switch their login region in Bambu Studio by going to Preferences -> Login Region.

Third-Party Account Login
Bambu accounts support linking with third-party accounts, which allows users to log in with a third-party provider. Currently:

- Domestic users can link their Bambu account with Apple, WeChat, Weibo, and QQ accounts.
- Overseas users can link their Bambu account with their Apple, Google, and Meta accounts.

Bambu accounts use the OAuth 2.0 (Open Authorization protocol), following its standard protocols and procedures for third-party login authorization. The security mechanisms of OAuth 2.0 ensure that Bambu account information is not disclosed to third parties.

4.2.2 Login Protection

Bambu accounts currently offer users the following two login protection measures: Two-Factor Authentication and one-click account logout.

Two-Factor Authentication (For Abnormal Login Attempt)
When a user logs in to their Bambu account with a password on a new device for the first time, they must complete two-factor authentication. This mechanism is an effective way to prevent user privacy data from being leaked if an account password is ever compromised.

One-Click Account Logout
If a user chooses to deactivate their account, all login sessions on previous clients will be simultaneously logged out. This reduces the risk of user account data being compromised.

4.2.3 User Data Security

Bambu Account Data Security Measures
When users register a Bambu account, the personal information they provide is encrypted and rigorously protected to ensure that data remains secure during both storage and transmission, preventing unauthorized access or misuse.

1. **Encrypted Storage of Personal Information**
   - Phone number or email: Before being written to the database, this information is encrypted using the AES-128 symmetric encryption algorithm, ensuring that even in the event of a database breach, the data cannot be directly accessed.
   - Password: Passwords are never stored in plaintext. Instead, they are processed using the industry-recommended Argon2 password hashing algorithm with the inclusion of a random salt. This approach provides strong resistance against rainbow table attacks and brute-force attempts.

2. **Key Management and Protection**
   - All cryptographic keys used for encryption are centrally managed by Key Management Service (KMS).
   - The KMS ensures secure storage and controlled usage of keys, preventing plaintext key exposure at the application layer.
   - Keys are subject to regular rotation, with emergency replacement mechanisms in place to mitigate the impact of potential key compromise.

3. **Access Control and Principle of Least Privilege**
   - Data access is governed by strict access control policies, allowing only authorized services or personnel to access the necessary information.
   - The system enforces the principle of least privilege, ensuring that each component or employee is granted only the minimum level of access required to perform their duties.
   - All data access activities are logged in audit trails, which are regularly reviewed by the security team.

4. **Security Testing and Compliance**
   - A dedicated internal security team continuously conducts automated security scanning and penetration testing to proactively identify and remediate vulnerabilities.
   - In addition to internal assessments, independent third-party security firms are periodically engaged to perform external penetration tests and security evaluations, ensuring alignment with industry best practices.
   - The system is designed and operated in accordance with international security and privacy standards such as ISO/IEC 27001 and GDPR, providing users with compliant and reliable data protection.

5. **Secure Transmission and Real-Time Protection**
   - Communication between users and Bambu cloud services is protected with TLS 1.2 and above, safeguarding against man-in-the-middle attacks and data interception.
   - The platform deploys real-time intrusion detection and prevention systems (IDS/IPS) to monitor for abnormal activities or attack patterns, enabling automatic response to reduce security risks.

4.3 MakerWorld Content Security

4.3.1 Content Review Rules

Bambu Lab has implemented a comprehensive content review for MakerWorld to ensure the platform is safe and respectful for all users. This review process covers a wide range of prohibited content and behaviors.

MakerWorld Content Review Focus Areas

- **Spam and Fraudulent Behavior:** This includes fake engagement, impersonation, duplicate content, and scams. The platform aims to prevent misleading information and intellectual property risks, such as using incorrect or irrelevant source model links or images from shopping websites or other users' models.
- **Sensitive Content:** MakerWorld prohibits content that endangers child safety, explicit or sensitive images in thumbnails, nudity and sexual content, content related to suicide and self-harm, and vulgar language.
- **Violent or Dangerous Content:** This category covers harassment and cyberbullying, harmful or dangerous content, terrorism and extremist speech, content from violent criminal organizations, and violent or graphic content in model listings, posts, or comments.
- **Offensive Speech:** Prohibited offensive speech includes abusing or defaming other platforms, using vulgar or obscene language, harassment, bullying, personal attacks, harmful slander against nations or ethnic groups, inciting racial or ethnic hatred, threatening the use of violence or harm, and promoting hate speech or behavior that encourages discrimination or intolerance.
- **Regulated Goods:** MakerWorld prohibits the sale of models that can be converted into firearms or explosives (with the exception of props or toys), illegal models or items, and content that promotes illegal or regulated goods, services, or transactions.

Violating these guidelines will result in the removal of the non-compliant content. Additionally, Bambu Lab has introduced stricter guidelines for print profile submissions, now requiring the upload of genuine photos of the completed print. This ensures quality and prevents the submission of profiles with obvious quality issues or mismatches.

4.3.2 Intellectual Property Rules

MakerWorld is a community that encourages creators to share freely while also placing a high value on intellectual property protection. For this reason, Bambu Lab has established and implemented a strict set of intellectual property management guidelines.

Reporting and Takedown of Models

Models can be taken down if they are reported by others or discovered by the platform.

- Community members can report models suspected of infringement.
- MakerWorld reserves the right to remove the relevant content and penalize the user without prior notification.

For more detailed community rules, please refer to the MakerWorld Official Community Guidelines: https://makerworld.com/en/community-guidelines

05
Privacy Compliance

At Bambu Lab, we deeply understand the growing value users place on privacy. Respecting and protecting every user's personal information is the cornerstone of our operations and our primary principle for building long-term user trust.

To turn this commitment into reality, we not only continuously listen to user feedback and improve our products with an open and collaborative attitude, but we have also established a dedicated Security Committee at the organizational level. This committee is devoted to building and perfecting a comprehensive Bambu Lab product security and privacy protection system. We are also actively seeking recognition from international authorities.

Through a series of rigorous evaluations and audits, we have successfully obtained multiple international privacy and security certifications. This serves not only as strong proof of our existing practices but also demonstrates our firm determination to continuously enhance our level of privacy and security protection.

5.1 Privacy Security Certification

Bambu Lab has obtained globally recognized information security and privacy certifications, underscoring our leadership in upholding internationally acknowledged security and privacy standards.

Below is a partial list of our information security and data privacy certifications:

5.1.1 ISO/IEC 27001

Bambu Lab was certified with ISO/IEC 27001 on April 11, 2025. This standard is a globally recognized and stringent information security management standard. This achievement signifies that Bambu Lab has fulfilled its commitment to its users and meets the requirements of international standards.

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

5.1.2 ISO/IEC 27701

Bambu Lab was certified with ISO/IEC 27701 on April 11, 2025. This standard, officially known as ISO/IEC 27701:2019, is the latest international standard developed specifically for privacy protection, and it integrates privacy practices into an information security management system.

This certification demonstrates Bambu Lab's commitment to upholding the best privacy protection practices.

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

5.1.3 TrustArc Enterprise Privacy

The TRUSTe certification is a privacy and data governance framework developed by TrustArc, an organization specializing in privacy protection. Bambu Lab obtained this certification in July 2025, which demonstrates that the company has established and implemented a privacy compliance management system aligned with internationally recognized standards.

5.2 Privacy Practice

5.2.1 Privacy Handling Principles

At Bambu Lab, our products and services are built on the following four fundamental privacy principles.

Privacy Principle	Description
Public Transparency	We strive to make our data handling practices public and transparent, empowering you to make informed choices.
Open Collaboration	We actively listen to user feedback, identify opportunities for privacy and security improvements, and continuously enhance our products and services.
User Control	We work to provide simple and intuitive methods to help you control your own information.
Privacy Compliance	Our privacy practices strictly adhere to current privacy and data security laws and standards, and they are validated through relevant certifications.

Table 2：Privacy Handling Principles

5.2.2 Privacy Policies

Bambu Lab places a high value on user privacy. Our Privacy Policy details our specific practices for collecting, using, disclosing, processing, and protecting your personal information that is provided or collected while you use our products or services.

We are committed to treating your data in a transparent and responsible manner, and we employ technical and organizational measures that align with industry best practices to protect your information security. To gain a more complete understanding of our privacy protection measures, please be sure to review our official Privacy Policy：https://bambulab.com/en/policies/privacy.

5.2.3 Data Storage Strategy

Bambu Lab has a flexible and secure global data storage strategy that fully accounts for different data protection regulations and user needs around the world. The location where user data is stored primarily depends on the user's geographical region. Specifically:

- **Mainland China Users:** User data is stored on Alibaba Cloud within Mainland China, in compliance with relevant Chinese laws and regulations.
- **Users in Other Regions:** For users located outside of Mainland China, data is currently stored in a data center on AWS in the United States. We implement strict data access controls and encryption measures to ensure data security.

In the future, we may adjust data storage locations due to business expansion or changes in local regulations. Any adjustments will comply with local laws and will be communicated to users in a timely manner. We are committed to providing secure and reliable data storage services to our global users.

If you have any privacy-related questions, please contact us at privacy@bambulab.com.

06
Open Source Plan

If we were to name the true heroes of 3D printing over the past decade, they would be the people behind Reprap, Marlin, Cura, Prusa, Slic3r, Hypercube, Voron, and Klipper. It is the open nature of the 3D printing community that has driven the development of desktop 3D printing. As a newcomer to the field, Bambu Lab has learned a great deal from our predecessors. Standing on the shoulders of giants has given us the opportunity for rapid development.

Because we have learned so much from the community, we have always maintained deep respect for the open-source 3D printing community and the broader open-source software community. For this reason:

- We have strictly complied with open-source licenses for all open-source code used in our products.

  > Open-source address: https://wiki.bambulab.com/en/knowledge-sharing/open-source-software

- As a small contribution back to the community, we have made extensive modifications to our slicing software, adding new algorithms, techniques, a project manager, and a clean user interface.

  > Open-source project URL: https://github.com/bambulab/BambuStudio

In the future, Bambu Lab will continue to strictly adhere to open-source licenses and contribute back to the community. We look forward to working hand-in-hand with more developers and enthusiasts to drive the progress of 3D printing technology.

07
Bug Bounty Program

The Bambu Lab Bug Bounty Program is a project that invites security experts to identify vulnerabilities in Bambu Lab's products and platforms and rewards them with corresponding bounties. The program is part of Bambu Lab's commitment to open collaboration with the industry to continuously improve product security and data privacy protection.

Over the course of more than two years, a total of 51 security researchers have participated in this program. To date, Bambu Lab has awarded cumulative bounties amounting to tens of thousands of U.S. dollars, along with multiple 3D printers, as recognition for their contributions. We sincerely thank these security experts for their efforts in helping Bambu Lab continuously improve product security and user privacy. We are well aware that ensuring the security of our 3D printers and our ecosystem requires continuous dedication and collaboration with the security community.

For more details on the program and bounties, please refer to:
https://bambulab.com/en/security

If you have any suggestions for the program, you can also provide feedback by emailing us at security@bambulab.com.

08
Conclusion

Bambu Lab is dedicated to providing innovative, efficient, and secure 3D printing equipment and solutions for individual, maker, and industrial users worldwide. As a core component of the Bambu Lab product experience, our firmware, software, and services bear the crucial responsibility of building user trust and ensuring device and data security. We will continue to advance our security technology, enhance the security and privacy protection features of our products and services, and constantly optimize our security and privacy management system. Through various channels, including technical documentation, white papers, privacy policies, and security audits & certifications, we will clearly demonstrate our security practices and commitments to users. This will help build confidence in our products and services, enabling users to more securely choose and use our innovative technology.

We firmly believe that only by fully respecting and protecting user data security and privacy can we earn lasting user trust. We will continue to increase our investment in this area, collaborate with the security community in an open and cooperative manner to enhance the security of our products and services, and listen to user feedback with a mindset of respect. Most importantly, we won't stop at listening; we will transform user concerns into tangible actions and integrate them into every aspect of product improvement. We believe that only through concrete effort and continuous optimization can we gradually earn the trust of our users.