PlugOS Security Whitepaper

Version：V1.1

Disclaimer

The content of this document will be updated periodically. This document is for use guidance only, and all statements, information, and suggestions contained herein do not constitute any explicit or implied warranties.

Contents

1. Foreword

1.1. Abstract

As data security incidents become more frequent and global privacy awareness continues to rise, the security of mobile and personal computing devices has become a central issue in the information society. Users are not only concerned about data theft by hackers and malicious applications, but also worried about the exposure of their privacy in scenarios such as forced searches or device loss. Traditional mobile devices, which are often driven by commercial and functional goals, struggle to guarantee users' data sovereignty.

PlugOS is a secure and private operating system running on independent portable hardware. With a core design philosophy of privacy-first, zero-trust, and minimize the trust boundary, it has built a multi-layered defense architecture covering hardware, kernel, system, and applications. This whitepaper discloses PlugOS's certifications, security threat model, security and privacy architecture, and security management. It provides technical experts, security managers, decision-makers, and all users concerned about digital rights with a transparent, verifiable, and auditable perspective. It aims to answer the most critical question: why PlugOS is worthy of users' reasonable trust.

1.2. Introduction

1.2.1 Background: Privacy and Security Challenges

In our highly connected digital age, personal data has evolved from a simple information carrier into a core asset driving business decisions and technological innovation. From daily consumption records and location trails to biometric and financial account data, it contains users' core interests. Mainstream operating systems often have a data-first tendency. In pursuit of commercial value, they often enable multi-dimensional data collection by default.

Mainstream operating systems use system permissions to obtain information like application usage duration and hardware details, and even merge fragmented data into user profiles for targeted advertising, product recommendations, or third-party sharing without explicit user consent. This passive collection model blurs privacy boundaries, and leads to an out-of-control data flow. Some data may flow to unauthorized institutions. Users are unaware of data usage and have difficulty revoking consent, severely weakening their privacy autonomy.

At the same time, users' data sovereignty faces multi-scenario, highly covert, and destructive threats. At the network level, mobile device attacks have advanced. Hackers use fake system updates, exploit vulnerabilities to implant malicious code, and use phishing to trick users into revealing sensitive information. In 2024, global mobile phishing incidents increased by 37% year-on-year, nearly 60% of them targeted high - value data such as financial and medical data. At the physical level, device theft and targeted attacks are common. Criminals dismantle hardware to extract unencrypted data, and supply chain vulnerabilities can lead to devices being monitored from the factory, over tens of millions of devices are affected.

Furthermore, coercion and social engineering attacks pose an invisible threat. Users may be forced to provide passwords or biometric information, while social engineering exploits psychological weaknesses to breach defenses. These intertwined threats lead to data breaches, financial losses, and even identity theft and reputational damage, highlighting the urgent need for a highly secure and privacy-protective system.

1.2.2 PlugOS: Redefining Data Sovereignty

PlugOS was created for the above challenges. PlugOS reconstructs an operating system based on security and privacy from first principles, rather than being a patchwork of incremental security features layered onto existing systems. It encapsulates a complete intelligent runtime, core applications, and user data within an independent portable hardware. By leveraging encrypted channels, PlugOS interacts with host devices (smartphones, tablets, or PCs) for I/O operations (display, input, and networking), and creates a verifiable, controllable, and physically isolated trusted execution environment. PlugOS breaks free from the data-harvesting inertia of mainstream operating systems. Through a defense-in-depth strategy spanning hardware → kernel → system → applications, PlugOS integrates privacy safeguards at every stage. This approach not only mitigates external threats, but also empowers users' right to know, right to control, and right to delete their personal data. PlugOS aims to be a guardian of user sovereignty rather than a conduit of data monetization.

1.2.3 Purpose and Target Audience

This whitepaper aims to provide a detailed technical explanation for technology experts, security managers, policymakers, and individual users who prioritize security and privacy. It will transparently demonstrate PlugOS's architecture and mechanisms, and elaborate on how it addresses various security challenges in the modern digital world. As this paper delves into professional fields like system security, cryptography, and hardware security, we assume the reader has a foundational knowledge of information security.

1.3. Terms and Definitions

The following terms and definitions apply to this paper.

Term	Abbreviation	Definition
Host Device	Host	The device (smartphone, tablet, or computer) that provides power and peripherals (e.g., screen, keyboard, touch, network) after PlugOS is inserted.
Host App / Companion App	Host App	The official application installed on the host device. It serves as the core bridge for the interaction between PlugOS and the host device. Main functions include: primarily responsible for forwarding peripheral capabilities, encrypted transmission of PlugOS output, and status monitoring and management.

Product Key	Product Key	A unique serial number and cryptographic credential written to each PlugOS at the time of manufacture, is used for device activation and secure binding with the host.
Secure Binding	Secure Binding	The mutual authentication process during the initial pairing of PlugOS and a host. It uses password verification and dynamic tokens to securely bind PlugOS to a specific host, preventing unauthorized host access.
Trusted Execution Environment	TEE	A secure area created on a computing platform through hardware isolation to ensure the confidentiality and integrity of code and data. A TEE is used to perform sensitive tasks in an isolated environment, such as privacy authentication and data protection.
Secure Element	SE	A physically independent, highly tamper-resistant dedicated microprocessor designed to store and process the highest level of confidential information, such as cryptographic keys.
Hardware Root of Trust	HRoT	A trust foundation established during the hardware manufacturing process that cannot be modified by software. It is the starting point for the entire system's secure boot and cryptographic operations.
Zero Trust Architecture	Zero Trust Architecture	A security model with the core principle of "never trust, always verify." It strictly authenticates and authorizes for any request to access resources, by default, does not trust the host or its app.
Attack Surface	Attack Surface	The sum of all possible entry points in a system that an attacker can exploit. A smaller attack surface generally means a more secure system.
End-to-End Encryption	E2EE	A communication encryption scheme that ensures data remains encrypted throughout its entire journey from the sender to the receiver, and can only be decrypted by the communicating parties.
Device Fingerprinting	Device Fingerprinting	A device fingerprint that uniquely identifies a device by collecting multiple software and hardware characteristics of the device, and it is often used to track users.
Sensor	Sensor	A technique that intercepts an application's access to

Virtualization	Virtualization	hardware sensors at the system level and provides user-controlled virtual data to counter device fingerprinting.
Duress Password / Duress Code	Duress Password / Duress Code	A security mechanism to deal with physical coercion scenarios. Entering this password either destroys data or leads to a "decoy system" with no real data.
Data Self-Destruction	Data Self-Destruction	A mechanism where the system automatically deletes all sensitive data (e.g., user files, keys, application data) when predefined conditions are met (e.g., user trigger, detection of a malicious attack, coercion scenario). The deletion is permanent and cannot be recovered by technical means. Under hardware self-destruction conditions, the device may become unusable.
Supply Chain Attack	Supply Chain Attack	Instead of directly attacking end-users, attackers exploit vulnerabilities in the product's supply chain (design, production, distribution) to implant malicious code.
Common Criteria Evaluation Assurance Level	CC EAL	A globally recognized standard for the security evaluation of IT products. A higher EAL level represents a higher degree of security assurance for the product.
Data Minimization	Data Minimization	One of the fundamental principles of privacy protection, which requires systems and organizations to collect and use only the minimum amount of personal information necessary to achieve a business goal.

2. Shared Security Responsibilities

In addressing the increasingly severe privacy and security challenges, PlugOS and its users must clearly define their respective security responsibilities. Both parties can jointly safeguard data sovereignty and privacy security by establishing a collaborative security system that combines technical guarantees with user protocols.

2.1. PlugOS's Security Responsibilities

PlugOS assumes core technical and compliance security responsibilities in its design and operation to ensure that the system itself is a trustworthy "secure foundation." This includes:

- **Technical Architecture Security:**
    - **Physical and Logical Isolation**: PlugOS is independent of the host system, and has

its own computing and storage capabilities to avoid data confusion with the host.

  - **Hardware-Level Protection**: It realizes implements execution and key protection through trusted components like TEE and SE; supports strong encryption and hash verification to ensure confidentiality and integrity.
  - **Resistance to Coercive Attacks**: Built-in mechanisms for brute-force attack clearing and duress password self-destruction to prevent data leakage caused by physical theft or coercion.

- **Providing Data Protection and Privacy Protection:**
  - Default minimal data collection, with no ads, no push notifications, and no listening.
  - Data is stored and processed locally to avoid risks of invisible uploads and cross-border data transfer.
- **Secure Operations and Compliance:**
  - Establishes a vulnerability monitoring and response mechanism, implements regular updates and patch fixes.
  - Promotes a bug bounty program to enhance security with the community and partners.
  - Ensures the system aligns with international and domestic security compliance standards (e.g., GDPR, PIPL, ISO/IEC 27001).
- **Users Support and Emergency Response:**
  - Provides technical security support and guidance.
  - Quickly assist in isolating risks and restoring a secure state when a Users encounters an emergency (e.g., device loss, suspected intrusion).

2.2. Users' Security Responsibilities

As the end-user of PlugOS, users play a crucial role in device management and usage. The users' security awareness and proper operation are key to maximizing the security effectiveness. The Users' core security responsibilities include:

- **Proper Management of Account and Device Credentials**: Properly keep device unlock passwords, product keys, and other critical credentials. Do not disclose account information to any third party. It is recommended to use strong passwords to enhance account security.
- **Cautious Permission and Application Authorization**: Configure system permissions based on actual needs and do not randomly authorize third-party applications to access sensitive data (e.g., location, contacts), doing so reduces the potential risks of social engineering attacks at the source.
- **Environmental Awareness and Operational Discipline**: When handing sensitive information by PlugOS, you need remain highly aware of the physical environment and check for hidden surveillance devices (e.g., cameras, recording devices). Avoid performing sensitive operations in complex or easily spied-on public areas (e.g., open offices, public transportation).
- **Ensuring Physical Device Security**: Although PlugOS has hardware-level tamper

resistance, users still need to properly keep the device to prevent loss, and avoid attackers from indirectly obtaining information through physical device or induced operations.

- **Keeping the System Updated and Responding Promptly**: Pay attention to security alerts and update notifications from PlugOS, and ensure the device always runs the latest secure version through timely device upgrades. In case of anomalies like device loss or suspected data breaches, you can contact the PlugOS technical team immediately to initiate the emergency response process and minimize risk.

3. Security Certifications and Compliance

PlugOS does not rely solely on self-proclamations, it builds a verifiable security standard through a triple guarantee of "**international authoritative certifications, alignment with global regulations, and participation in industry standards.**" We adhere to a philosophy of "external independent verification + internal continuous improvement" to ensure the long-term trustworthiness of PlugOS globally. This section will introduce the certifications we have obtained, the laws and regulations we follow, and our contributions to industry standards.

3.1. International System Certifications

We strictly adhere to international authoritative standards in the establishment of our R&D and management systems. Rigorous security considerations are integrated into every step, from requirements analysis and architecture design to development and testing. We have obtained multiple third-party authoritative certifications, including: ISO/IEC 9001:2015, ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO/IEC 29151:2017, and CMMI Level 3. We possess mature, standardized, and sustainable capabilities in information security, privacy protection, and software engineering management, which lay a solid foundation for the outstanding security performance of PlugOS.

3.1.1 ISO/IEC 9001 (Quality Management System Certification)

ISO/IEC 9001 is a global standard for quality management systems jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It focuses on three core concepts: Users focus, process approach, and continuous improvement, and provide organizations with a systematic framework for quality management to ensure that products/services consistently meet Users needs and regulatory requirements throughout their lifecycle.

ISO/IEC 9001 is the cornerstone of PlugOS's quality management. By integrating the standard's requirements into the entire process of R&D, production, delivery, and service, PlugOS has achieved the goals of stable security functions, consistent product experience, and efficient response to user needs. We provide a security and high-quality operating system solution for users.

3.1.2 ISO/IEC 27001 (Information Security Management System Certification)

The Information Security Management System standard (ISO/IEC 27001) is jointly developed by ISO and IEC and is a globally recognized authority in the field of information security management. It plays an irreplaceable role in protecting information resources and promoting the healthy development of information technology. It can effectively protect information resources and ensure a healthy, orderly, and sustainable information technology process.

ISO/IEC 27001 specifies various requirements and best practices for information security management, we comply with the security framework for PlugOS's R&D management. It ensures that all links comply with information security, and help the organization meet information security compliance requirements to avoid legal risks and reputational damage from non-compliance.

3.1.3 ISO/IEC 27701 (Privacy Information Management System Certification)

ISO/IEC 27701 is an international standard jointly developed by ISO and IEC. It is an extension of the ISO/IEC 27001 Information Security Management System standard. It focuses on privacy information management. It provides a systematic and operable framework for organizations to protect personal information, and its requirements are deeply aligned with major global privacy regulations (China's PIPL, the EU's GDPR, the US's CCPA/CPRA, Brazil's LGPD, etc.).

We have used ISO/IEC 27701 to review the entire lifecycle management process of personal information of PlugOS, establish a standardized privacy risk control mechanism, eliminate management blind spots, and continuously optimize.

3.1.4 ISO/IEC 29151 (Code of Practice for the Protection of Personally Identifiable Information)

ISO/IEC 29151 is an international standard jointly published by ISO and IEC regarding the protection of personally identifiable information. It focuses on the code of conduct that personal information processors should follow when handling such information. The goal is to enhance the protection of personally identifiable information, thereby safeguarding the privacy rights of the public. It plays a significant role in the global digitalization process.

PlugOS strictly implements this standard, and regulates the collection, storage, processing, use, and disclosure of personal information to protect users' privacy rights.

3.1.5 CMMI Level 3 Certification (Capability Maturity Model Integration Level 3)

CMMI (Capability Maturity Model Integration) is a globally recognized standard for evaluating an organization's capabilities in project management, engineering development, and process management. CMMI Level 3 (Managed Level) is a key milestone for an organization to shift from passive reaction to proactive control. Organizations are standardized and can consistently deliver high-quality results based on Level 3.

The R&D and design of PlugOS are guided by the CMMI. We have benchmarked CMMI's requirements for standardized processes, compliant execution, and reusable assets. The entire lifecycle of PlugOS complies with Level 3, from requirements analysis and architectural design to development, testing, and operational maintenance. This guarantees the product's security, stability, and scalability.

3.2. Product Security Certifications

The security of PlugOS is built on hardware components that have been verified by the industry's most stringent standards. The hardware components have passed the CC (Common Criteria) certification system. The CC (Common Criteria for Information Technology Security Evaluation) is the most authoritative and widely used standard for evaluating the security of IT products and systems globally. It enables mutual recognition of security evaluation results across different countries and regions and help businesses and organizations to choose secure products for a more reliable option.

3.2.1 TEE OS Security Certification

The TEE OS built into PlugOS, as a key defense for system security, has successfully passed the CC EAL4+ security certification. This not only proves its ability to resist common attacks, but also demonstrates its security and reliability in large-scale commercial scenarios. This is a vital assurance of our technical strength and user security experience.

This TEE OS has also been validated through mass production of over a billion devices. This large-scale production experience verifies the technical reliability of the TEE OS and proves its feasibility and stability in large-scale commercial applications. We have full confidence in the security performance of PlugOS.

3.2.2 SE Security Certification

The independent Secure Element (SE) component used in PlugOS builds an unbreakable security barrier for users with its outstanding security features. This chip has been awarded CC EAL6+ security certification, which is a high-level status in the global security standard system for various application scenarios.

The CC EAL6+ certification ensures that this chip component can operate stably in complex financial environments. Whether PlugOS is used for core banking transactions or for protecting sensitive information like user payment passwords and transaction records, it delivers reliable security, enabling users to enjoy digital financial services with peace of mind.

3.3. Alignment with Global Laws and Regulations

PlugOS practices the principles of "**Privacy by Design**" and "**Data Minimization**." We do not collect, process, or store any user-identifiable data. This architectural design makes it inherently compliant with the core requirements of major global data protection regulations, such as China's PIPL, the EU's GDPR, and the US's CCPA.

3.3.1 People's Republic of China Personal Information Protection Law (PIPL)

PIPL is China's first comprehensive law enacted to protect the rights and interests of individuals' personal information, standardize personal information processing activities, and promote the reasonable use of personal information. The law explicitly states that the personal information of natural persons is protected by law, and no organization or individual may infringe upon the rights and interests of a natural person's personal information. Activities involving the processing of personal information of natural persons within China are subject to its constraints.

PlugOS's design and features are fully aligned with the requirements of this law. From a design perspective, PlugOS adheres to the principle of "Privacy by Design," firmly rejecting data collection and behavioral analysis. The system has no ads, no recommendations, no listening, and no uploads, fully respecting an individual's right to control their own information. This is fully consistent with the PIPL's provision that personal information handlers must follow the principles of legality, propriety, and good faith.

3.3.2 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is the EU's highly influential data protection regulation. It not only has a profound impact on organizations within the EU, but also requires all enterprises worldwide that are involved in the processing of EU personal data to adjust their data management strategies to ensure compliance. GDPR has set a benchmark in the field of global data protection, and significantly changes how enterprises process personal data to advance personal data protection to a new level.

PlugOS fully complies with the strict requirements of the GDPR. We adhere to the "Privacy by

Design" philosophy, eliminating data collection and behavioral analysis. Its independent Secure Element (SE) or Trusted Execution Environment (TEE) components provide hardware-level encryption for storage, secure boot, and tamper resistance to ensure data security and confidentiality. The self-destruct mechanism can quickly destroy data to prevent leaks, comprehensively protecting user data rights.

3.3.3 California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) is a state law in California, USA. It is enacted to enhance the privacy rights and consumer protection of its residents. As the first comprehensive data privacy legislation in the US, CCPA aims to give California residents greater control over their personal data to build a solid legal barrier for consumer privacy and data security.

In the trend of data privacy protection, PlugOS strictly complies with the requirements of the CCPA. In its design, it eliminates data collection and behavioral analysis, with no ads, no recommendations, no listening, and no uploads, fully respecting consumers' right to control their personal information. This aligns with the core spirit of the CCPA to empower consumers. In its functional implementation, the TEE and SE play key roles, meeting the CCPA's requirements for information confidentiality. Data protection employs AES encryption and key management mechanisms to ensure confidentiality, and uses hash algorithms to verify integrity—thus meeting the CCPA's requirements for information quality. In addition, its support for brute-force attack clearing and duress password self-destruction mechanisms enables the active destruction of information in high-risk scenarios, effectively protecting consumers' information rights and fully complying with the CCPA's requirements.

3.4. Industry Standard Setting and Contributions

We are committed to advancing the improvement of information security industry standards and have been deeply involved in the development of multiple key security standard specifications. This includes:

- **Industry Standard:** "Technical Requirements for eSIM Based on Trusted Execution Environment (TEE)" (YD/T 6153-2024).
- **Group Standards:** "Technical Specification for Financial Security Chip Central Processing Units" (T/BFIA 007—2021) and "Information Security Technical Requirements for Digital Car Keys in Mobile Smart Terminals" (T/TAF 074—2020).

By participating in standard-setting, we not only contribute our technical insights to the industry, but also integrate these high-security requirements into the PlugOS technical architecture from the outset, anchoring our product to the highest security benchmarks in the industry.

3.5. Independent Third-Party Security Audits and Internal Compliance Management

PlugOS has established a dual-track compliance mechanism: "external independent verification + internal continuous improvement."

- **External Independent Verification:** We regularly hire top-tier, independent third-party security firms to conduct comprehensive penetration testing and source code-level security audits of the PlugOS operating system, hardware design, cryptographic implementations, and the host companion app.
- **Internal Compliance Loop:** We have established a professional compliance management team that dynamically tracks changes in global regulations and standards. We conduct a full-process compliance internal audit at least every six months to ensure that management, R&D, and delivery processes, thereby continuously enhancing the effectiveness of PlugOS's compliance program.

4. Security Threat Model and Design Principles

A sound security system begins with a deep understanding of threats and a clear design philosophy. The security threat model is the foundation of PlugOS security design. By defining "what to protect," "who to defend against," "how to delineate the trust boundary," and "what cannot be solved," it clearly defines the core scope of security protection.

4.1. Core Protected Assets

PlugOS is designed to protect data and applications stored on or run in PlugOS. These assets include but are not limited to:

- **Keys and Credentials**: Cryptographic keys, authentication tokens, various account passwords, etc.
- **User Private Data:** Files, message records, contacts, calendars, photos, audio, and video, etc.
- **Communication Metadata and Content:** The communication behavior itself, session content, relationship graphs, etc.
- **Financial Assets and Identity Credentials:** Digital currency private keys, online banking credentials, digital identity certificates, etc.
- **Location and Behavioral Trails:** Geographic location information, application usage records, network access history, etc.

4.2. Defensive Subjects (Attacker Model)

PlugOS's defense model covers multi-dimensional and multi-layered attacker types, including but not limited to the following common types:

- **Physical Coercers:** Individuals who attempt to force a user to unlock a device and hand over credentials under physical duress or pressure. For example, if a user is hijacked, resisting could endanger their life, while complying means the attacker will steal both their financial assets and privacy.
- **Physical Attackers:** Technicians who, after a device is lost or stolen, attempt to extract data from the device using physical means such as Cold Boot Attacks, JTAG debugging,

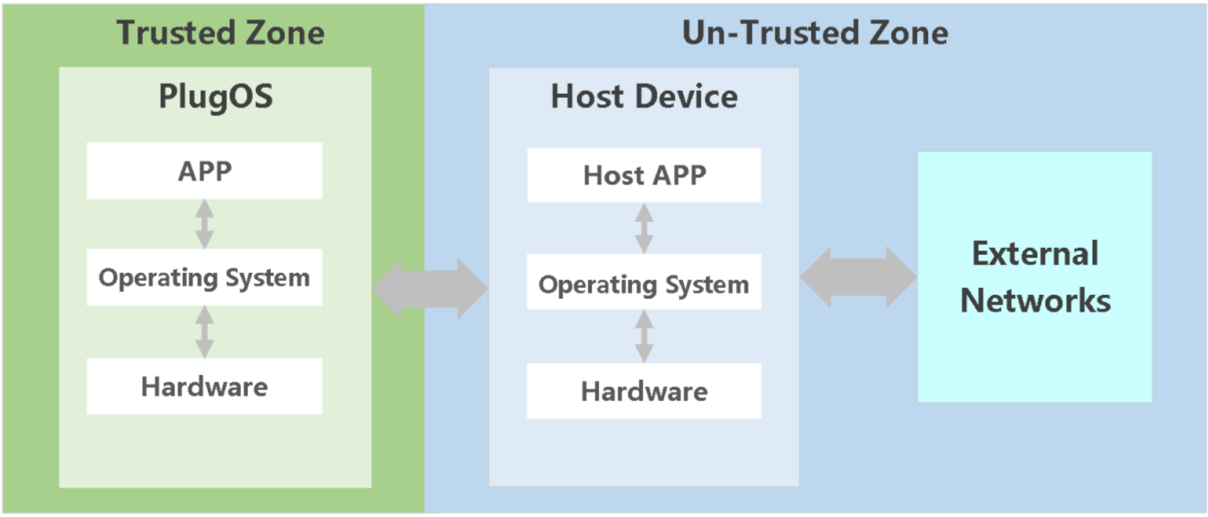
or Chip-off Forensics. After a device is stolen, the attacker attempts to extract data from PlugOS through these methods.

- **Supply Chain Attackers:** Internal or external personnel who attempt to implant hardware backdoors, malicious firmware, or contaminated software packages during the device's production, transportation, distribution, or software update stages.
- **Host Intruders:** Attackers who gain full control of the host device (PC or phone) to which PlugOS is connected and attempt to attack PlugOS through host-side malware.
- **Malicious Application Providers**: Attackers who trick users into installing malicious applications on PlugOS, attempting to steal data from other applications, perform unauthorized operations, or establish a covert channel.
- **Network Attackers:** Attackers who attempt to eavesdrop on or tamper with PlugOS network communications through Man-in-the-Middle (MITM) attacks, DNS hijacking, malicious Wi-Fi hotspots, etc.

4.3. Trust Boundary (Zero Trust)

"Zero Trust" is PlugOS's core security philosophy, which means it does not trust any network, external application, or neighboring system by default. The trust boundary is explicitly and minimally defined to reduce the system's attack surface.

- **Trusted Zone:** The PlugOS hardware device, its firmware, and the operating system that has passed signature verification. All user data and applications run in this zone.
- **Untrusted Zone:** The host operating system, the host companion app, and all external networks.



Trust Boundary Diagram

A clear, hardware-enforced security boundary exists between the Trusted Zone and the Untrusted Zone. The two only interact through a limited, end-to-end encrypted I/O channel. The table defines the responsibilities and permissions of the two:

Dimension	Trusted Zone (PlugOS)	Untrusted Zone (Host Device)

Runtime Environment	Independent hardware + TEE/SE + Secure OS.	Host open OS (e.g., Android/ iOS/ Windows).
Permission Scope	Manages all internal applications and data, with hardware-level encryption and isolation capabilities.	Acts only as an I/O proxy; has no permission to access any plaintext data inside PlugOS.
Data Storage	Hardware-encrypted storage for user data; data circulates in an internal closed loop.	Only stores non-sensitive configuration data; no user data is stored
Security Responsibility	Undertakes the responsibility for the entire lifecycle security and privacy of user data, covering storage, computation, and destruction.	Only ensures the integrity of its own code and the security of related channels; does not participate in core security decision-making.

4.4. Unsolvable Security Threats

To maintain transparency, we must clearly point out the security risks that PlugOS's threat model cannot directly cover. These risks mainly stem from factors outside the trusted zone, and their mitigation depends on the user's security awareness and behavior. There are two main categories.

4.4.1 Risks Arising from User Errors

PlugOS is designed to prevent unauthorized access but cannot prevent unsafe operations performed actively or inadvertently by users. This includes:

- **Social Engineering and Phishing Attacks:** Users are tricked into clicking malicious links, downloading malicious attachments, or actively entering credentials on fake websites.
- **Credential Leakage:** Users actively disclose high-privilege credentials (e.g., unlock passwords, product keys) to others, or store them in an insecure location, leading to leakage.
- **Malicious Application Authorization**: Users actively install an unknown application on PlugOS and grant it excessive permissions.

Mitigation: While PlugOS provides technical protection through mechanisms such as least privilege, application isolations, and a network firewall, the final line of defense remains the user's security awareness. We strongly recommend that users only install applications from trusted sources and prudently grant permissions. For additional guidance, see Chapter 11, "User-Operable Security Verification Checklist."

4.4.2 Risks Arising from Untrusted Environments (Host and Physical Environment)

PlugOS's security boundary ends at its physical hardware. There may be a risk of information leakage, when the external physical environment or connected host environment is completely controlled by an attacker.

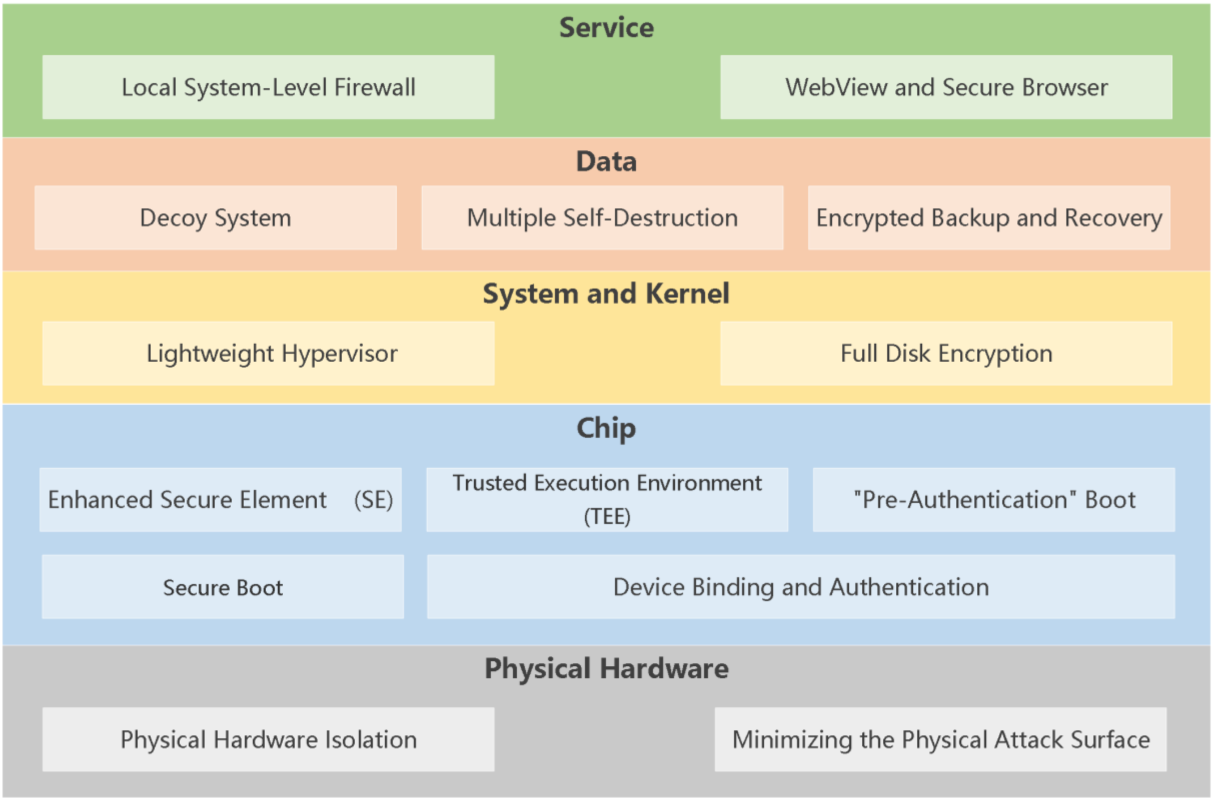
- **Physical Environment Eavesdropping**: Attackers may use hidden cameras, shoulder surfing, or similar methods to steal information when users enter a password or view the screen. This is beyond the protection capabilities of any endpoint device itself. It is recommended that users ensure the security of their physical environment when handling sensitive information.
- **Fully Compromised Hosts:** PlugOS is designed to ensure that even if a host is infected with malware, the malware cannot directly access static data (Data-at-Rest) or runtime data (Data-in-Use) inside PlugOS. However, data must be routed through the untrusted host for I/O operations when it is being displayed (Data-in-Display) and input (Data-in-Input). Therefore, a host fully controlled by kernel-level malware (e.g., advanced keyloggers, low-level screenshot tools) could theoretically record users' keyboard input and on-screen display content.

Mitigation: This is an architectural choice that balances security, portability, and cost-effectiveness. The PlugOS host companion app includes built-in runtime environment security detection capabilities, which can effectively counter most application-level screen capture, recording, and injection attacks. However, against kernel-level attacks on the host operating system, no application-level protection can provide an absolute guarantee. Therefore, we recommend that users connect PlugOS to a host device that they own, control, and maintain in a good security state to minimize this risk.

5. Security Architecture

PlugOS's security architecture adheres to the core principle of defense-in-depth. It takes a tamper-proof Hardware Root of Trust as its foundation and constructs a fully connected trusted computing environment from the chip to the application layer through layered, interlocking security mechanisms. We not only adopt and enhance the mature security model of AOSP (Android Open-Source Project) but also strive to counter extreme threats—from physical intrusion and supply chain attacks to forced coercion—through architectural innovation, ensuring the confidentiality and integrity of user data.

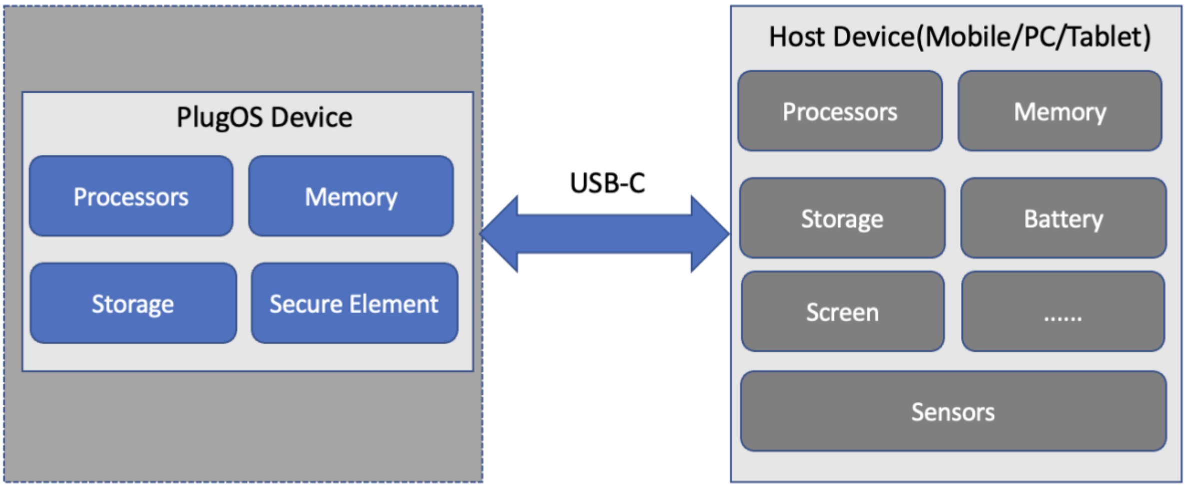
This section will analyze PlugOS's core security mechanisms one by one, covering physical hardware, chips, the system kernel, data, and core services. The goal of these mechanisms is to provide architecture-based, verifiable security, rather than security based on promises.


Service
Local System-Level Firewall
WebView and Secure Browser
Data
Decoy System
Multiple Self-Destruction
Encrypted Backup and Recovery
System and Kernel
Lightweight Hypervisor
Full Disk Encryption
Chip
Enhanced Secure Element (SE)
Trusted Execution Environment (TEE)
"Pre-Authentication" Boot
Secure Boot
Device Binding and Authentication
Physical Hardware
Physical Hardware Isolation
Minimizing the Physical Attack Surface

PlugOS Security Architecture Diagram

5.1. Physical Hardware Isolation and Attack Surface Minimization

This is the first and most intuitive line of defense against external threats.



Hardware Component Architecture Diagram

Physical Hardware Isolation: PlugOS is a complete, independent computing and storage unit, equipped with its own high-performance processor, high-speed memory, and large-capacity storage. It is physically isolated from the host system (i.e., the user's computer or phone). This means the host operating system cannot architecturally access PlugOS's memory address space or storage chip. Even if the host is fully compromised by malware, it cannot cross this physical boundary.

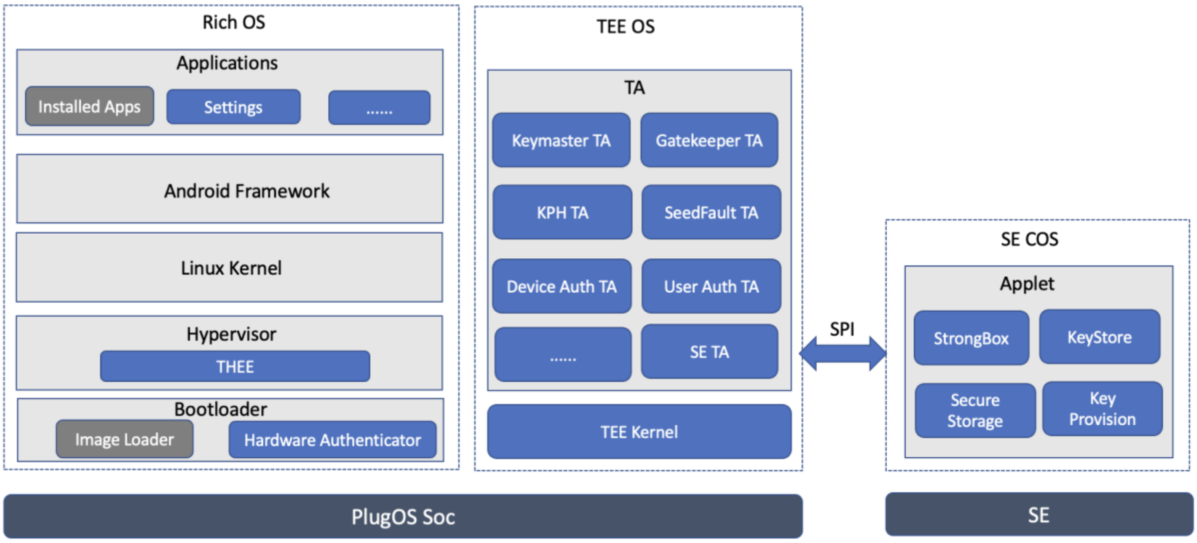
Minimizing the Physical Attack Surface: PlugOS's hardware design adheres to a minimalist principle. The device excludes complex radio frequency (RF) components such as cellular basebands, NFC, and GPS, as well as unnecessary sensors. It only interacts with the outside world via a single USB-C interface protected by a robust encryption protocol. This design significantly reduces the physical and software attack surface, mitigating the risk of remote or close-range attacks at the source.

5.2. Chip-Level Security Isolation

Hardware is the starting point for all security. PlugOS's security model begins with a hardware-enforced, tamper-resistant Hardware Root of Trust.

5.2.1 Chip-Level Security Isolation Foundation

The security isolation of PlugOS is built on the Secure Element (SE) chip and Trusted Execution Environment (TEE), ensuring that critical operations cannot be tampered with.



PlugOS Chip Isolation Architecture Diagram

Enhanced Secure Element (SE): Some PlugOS models include a built-in independent SE chip with CC EAL6+ certification. The SE is a compact secure computer with physical tamper resistance, providing "physical safe-level" protection for core confidential information such as cryptographic keys. CC EAL6+ is among the highest-level chip security certifications available today. By deeply integrating the SE's capabilities, PlugOS natively supports the Android StrongBox Keymaster specification, ensuring that key generation, storage, and usage are completed entirely within the hardware and inaccessible to any external software—including the operating system. This delivers hardware security guarantees for cryptographic operations and credential management on par with those of a bank card chip.

Trusted Execution Environment (TEE): All PlugOS devices are equipped with a TEE based on ARM TrustZone technology. Its TEE OS core, provided by industry leader TrustKernel, has passed CC EAL4+ security certification and been validated through mass production in over a billion devices. The TEE creates a hardware-isolated runtime environment parallel to the main operating system, supporting PlugOS's dual-factor authentication (user and device), data encryption/decryption, key management, and SE management. This effectively prevents vulnerabilities in the main operating system from impacting core security functions.

5.2.2 Architectural Innovation: "Pre-Authentication" Boot Process

PlugOS subverts the traditional "post-boot authentication" model. While traditional Secure Boot can verify the integrity of system signatures, it cannot prevent backdoored firmware from executing prior to user authentication. For instance, many commercial cracking tools can physically bypass security measures and extract user data from a device without authorization—primarily by exploiting vulnerabilities in the device's low-level firmware. PlugOS addresses this issue at the architectural level: before any system code is loaded, verified, or executed, the device must complete dual-factor authentication (of both the user and the host device) at the chip level. **This thwarts traditional methods of bypassing authentication defenses via physical attacks, supply chain tampering, or low-level firmware vulnerabilities.** For example, even if a backdoor exists in the chip firmware or Linux kernel layer, the backdoored supply chain firmware will never be powered on or executed unless dual-factor authentication (of the user and device) has been completed via the hardware security chip.

Secure Boot: Every stage of the device's boot process is verified via a digital signature, forming a complete "chain of trust." Any unauthorized firmware or tampered system image will not be loaded or executed—this is because the disk decryption key it relies on is not present in memory until authentication is successful.

Device Binding and Authentication: PlugOS only allows connections to authenticated and authorized host devices. When used with a host for the first time, the user must bind the host using the product key of the PlugOS device. For subsequent connections, only hosts that have been bound and verified will be recognized. Host authentication is based on identifying the host's physical hardware features. After the initial binding, PlugOS generates a binding key pair for the host, which serves as the authentication factor for subsequent connections. This prevents man-in-the-middle (MITM) attacks and unauthorized access.

5.3. System and Kernel-Level Security Hardening

Based on hardware guarantees, PlugOS builds a strong software isolation defense through advanced virtualization technology and mandatory encryption mechanisms.

Kernel Isolation based on a Lightweight Hypervisor: In a traditional monolithic kernel architecture, once an attacker gains root privileges, the entire system is fully compromised. PlugOS features a self-developed lightweight hypervisor (virtual machine monitor) that virtualizes and isolates critical components of the operating system kernel (e.g., memory management components, security policy management components). It creates an independent security domain for each application with strict policy restrictions. This design makes it difficult for vulnerabilities in a single application or system service to spread laterally, limiting the scope of the vulnerability's impact on the kernel or other applications and enhancing the system's anti-penetration capabilities.

Full Disk Encryption (Encryption on Write): PlugOS enables file-level full disk encryption by default. Any data written to the storage medium is automatically encrypted by the hardware encryption engine at the moment of writing. Each file is encrypted with an independent key, and these file keys are protected by a master key. This master key is securely stored in the TEE/SE and strongly bound to the user's unlock credentials. This means that even if an attacker physically obtains the flash memory chip (e.g., through chip-off forensics), they cannot read any valuable plaintext information.

5.4. Data Self-Destruction and Secure Recovery

In addition to a robust traditional security architecture, PlugOS has innovatively introduced data protection mechanisms for extreme scenarios such as physical coercion and brute-force attacks. This forms the last line of defense for user data security, ensuring users maintain absolute control over their own data.

To counter extreme coercion or physical cracking, PlugOS features built-in multiple data self-destruct mechanisms. These mechanisms can be triggered by consecutive incorrect password entries or when a user actively enters a preset duress password on the unlock screen. Once triggered, the system irreversibly destroys the encryption keys, instantly rendering all data on the disk unrecoverable. Additionally, PlugOS provides an end-to-end encrypted backup and recovery solution. Users can securely back up their data to a trusted storage location of their choice, with the encryption key remaining under their control. This ensures autonomous storage and recovery capabilities, with data sovereignty retained in the user's hands.

5.4.1 Duress Password

- **How It Works:** Users can preset a duress password. When this password is used to unlock the device, PlugOS will seamlessly delete all internal data.
- **Use Case:** In a situation where users are forced to unlock the device, they can use the duress password to protect their safety and real data, presenting a worthless target to the attacker.

5.4.2 Self-Destruct Mechanism

- **Trigger Conditions:**
  - Anti-Brute Force: The number of consecutive incorrect password entries reaches a ser-configured threshold.
  - Physical Tamper Resistance (some models only): Detection that the device's casing has been opened or a critical chip is under physical attack.
  - Duress Password Trigger: Users can configure a duress password to trigger silent self-destruction.

- **Execution Process:** Once triggered, the TEE or SE executes an irreversible encryption key destruction process, instantly rendering all encrypted data into unrecoverable gibberish and thereby achieving a complete erasure of all sensitive data.

5.4.3 Encrypted Backup and Recovery

The end-to-end encrypted backup and recovery capabilities provided by PlugOS ensure that all your data remains encrypted during backup, transmission, and recovery, maximally preventing unauthorized access. Backup data is end-to-end encrypted on the device using a key known only to the user before it is exported to a user-selected storage location (e.g., personal computer, external storage device, etc.). The recovery process also requires the user to provide the key to complete the decryption locally. As a service provider, we cannot access any plaintext content of the user's backup throughout the process, ensuring the integrity of user data sovereignty during backup and recovery.

5.5. Critical Service Security Enhancements

PlugOS has deeply re-engineered and enhanced several core system services that are closely related to privacy and security. For example:

Local System-Level Firewall: As one of PlugOS's core network security components, the firewall is deeply integrated with the system's network stack, enabling it to enforce access control over all application (including system applications) network activities. It runs locally, does not share or upload any logs, and can identify and block built-in application trackers and telemetry connections. Users can formulate fine-grained network access policies based on applications, domain names, IP addresses, and ports, truly achieving full control over every connection.

WebView and Secure Browser: PlugOS's built-in browser and in-app WebView components are based on Chromium and integrate enhanced patches from several leading security projects. We have removed all dependencies on Google services and telemetry code, disabled high-risk Web APIs by default, enabled strict cookie isolation and tracking protection policies, and strengthened the JIT compiler to defend against memory-based attacks. This provides users with a clean browsing environment that does not collect data, track activity, or cause disturbances.

6. Privacy Architecture

In contrast to mainstream operating systems' default data and behavior collection with an optional opt-out model, PlugOS strictly adheres to the core principle of "Privacy by Design." We do not build a safer advertising platform; we architecturally eliminate any form of unnecessary data collection instead. All of PlugOS's mechanisms revolve around three goals: **data localization, non-analysis of behavior, and full user control**, ensuring that every digital action a user takes serves only their own intentions.

This section will detail the core privacy technologies PlugOS has built to achieve these goals.

6.1. Zero Data Collection

In traditional mobile operating systems, even if users disable most data sharing options, system-level background telemetry and behavioral analysis still persist. This invisible collection is often used to optimize services or for targeted advertising, but it fundamentally weakens the user's privacy sovereignty. Zero telemetry and data localization are the cornerstones of the PlugOS privacy commitment: we do not collect your data because our system is not designed to do so.

- **Telemetry and Analytics Disabled by Default**: PlugOS is built on AOSP, but during the compilation and customization process, we systematically remove or disable all Google service frameworks and AOSP's built-in telemetry, crash reporting, and user behavior analysis components from the system layer to the framework and core application layers. In PlugOS, there are no background services that send your application usage habits, system performance data, or personal preferences to the device manufacturer or software developer.
- **No Ads, No Recommendations**: Since there is no user profiling or behavioral analysis, the PlugOS system globally contains no ads or personalized recommendation content. The user's digital experience is guided by their own will, not by algorithms.
- **Data Localization and Minimization Principles**: Our philosophy is that data that is not stored is the safest data. We have redesigned the system itself and all its built-in basic applications (e.g., browser, keyboard, file manager) to strictly follow the principles of data localization and minimization. For example, our keyboard only processes user input locally on the device and does not perform any form of cloud suggestion or user dictionary upload.
- **Zero-Knowledge Model**: Even the system manufacturer and TrustKernel cannot access any sensitive user data through PlugOS. All user information remains in the user’s own hands, and the manufacturer’s role is limited to providing a secure tool.

Traditional systems such as Android and iOS, even with ad tracking restrictions enabled, still upload some anonymized data via telemetry. PlugOS, by contrast, has no such restriction switch—this is because data collection does not exist in the first place.

6.2. Sensor Virtualization: Blocking Hardware Fingerprint Tracking

Modern applications widely use Device Fingerprinting to identify and track users. These fingerprints typically combine hundreds of parameters from hardware features (e.g., IMEI, sensor ID, baseband information), network environment (IP address, DNS, time zone), and software status to create a unique user and device identifier. Even if a user changes accounts or clears the cache, it is difficult to avoid re-identification and continuous tracking. Device fingerprinting generally does not require special permissions, and users are often unaware of it, which can continuously lead to the leakage of private information and tracking of their behavioral patterns.

Through system-level sensor virtualization, PlugOS cuts off the path of device fingerprint generation, thereby effectively protecting personal identity and behavioral privacy.

6.2.1 Identity Identifier Virtualization

For hardware IDs that can serve as unique identifiers, PlugOS implements virtualization. When applications request such information, the system selectively provides either generic, meaningless default values or different random values for different applications rather than real hardware serial numbers, SIM card information (IMSI/ICCID), MAC addresses, and the like.

6.2.2 Sensor Data Simulation

Users can simulate various environmental information through a centralized privacy control panel to provide false but plausible data to applications to meet their operational needs while protecting real information. For example:

- **Virtual Geographic Location**: Users can set a fixed virtual location or a dynamic virtual travel path.
- **Virtual Network Status**: Simulate different cellular network operators, network types, and cell tower information.

6.2.3 Dynamic Hardware Passthrough Switching

When needed, users can, with permission confirmation, pass the host's real hardware (camera, microphone, Bluetooth) directly to a specific application inside PlugOS, flexibly switching between functionality and privacy protection. Users can revoke authorization at any time, ensuring that hardware access is on-demand and turned off when not in use.

This design ensures that even the most aggressive fingerprinting algorithms find it difficult to establish a reliable identity link, thereby maximizing the anonymity and de-identification of the user and device.

6.3. Transparent and Controllable Network Connections

Network traffic is a major channel for data leakage. Many applications upload logs, SDK data, or behavioral information to third-party servers without notifying the user.

PlugOS has a built-in system-level firewall that gives users unprecedented insight and control over network traffic, allowing them to know, control, and trace every data connection. Its core tool is the kernel-level firewall mentioned in Chapter 3; this section focuses on its privacy protection functions.

- **Tracker Identification and Blocking:** The built-in database can detect common advertising SDKs and analytics SDKs in applications and alert the user to the potential privacy risks of the connection. The user can choose to block these third-party trackers.
- **Connection Auditing:** The firewall records all network connection requests from applications in real-time and presents them to the user in a clear, easy-to-understand way, including the destination domain name, IP, and protocol. This prevents covert data uploads

and exposes data exfiltration behavior hidden behind applications. The user can choose to block network connections for certain applications or destination servers.

- **Whitelist Mode:** For scenarios involving highly sensitive data, users can enable a strict "whitelist" mode, which by default prohibits all network connections and only allows access to specific domain names or IP addresses manually approved by the user. For scenarios where network access is completely unnecessary, users can cut off all network permissions with a single click, eliminating any possibility of information leakage.

7. Host Companion App

The host companion app is the companion application for PlugOS on mobile devices or computers. Its primary function is to enable PlugOS to use the host's peripherals—such as the screen and keyboard—for interaction and display. This section will clarify, from the perspectives of its role, responsibilities, and boundaries, that this app will not become a security risk vector for PlugOS.

7.1. Core Role: A Limited "I/O Proxy"

The host companion app is designed to strictly adhere to the principles of least privilege and zero trust. Within PlugOS's security model, it is explicitly categorized in the "Untrusted Zone" (see Section 4.3). Its core role is that of a limited "I/O Proxy," serving as a bridge between the user and the PlugOS hardware device. In other words, even if the host companion app contains vulnerabilities, is tampered with by a hacker, or is fully compromised, it cannot access or decrypt data stored within PlugOS.

7.2. Responsibilities and Limitations: What It Can Do and Cannot Do

To clearly define its capabilities, the following table lists the allowed responsibilities and the architecturally restricted behaviors of the companion app:

Allowed Responsibilities **(What it can do)**	**Architecturally Restricted Behaviors** **(What it cannot do)**
1. Forward Input: Receives keyboard, mouse, touch, and other input signals from the host and forwards them unaltered to the PlugOS hardware through an end-to-end encrypted channel.	1. Decrypt Any Data: All encryption keys are securely stored in the PlugOS hardware's TEE/SE and never leave the hardware. The app cannot obtain the keys, so it cannot decrypt any data it transmits.
2. Render Output: Receives screen image frame data streams from the PlugOS hardware and renders them on	2. Access Plaintext Data: The app serves only as a channel for PlugOS to communicate with the outside world. It cannot know the specific content

the host's screen for display.	of network communications.
3. Proxy Encrypted Network: Acts as a network egress, forwarding encrypted network traffic from PlugOS to the internet.	3. Execute Core Logic: All core computing tasks, such as user authentication, data encryption/decryption, file system read/write, and application execution, are completed independently within the PlugOS hardware. The app does not participate in any decision-making process.
4. Check for its own updates: Connects to the official server to check for new versions of the app, without involving any user data interaction.	4. Store User Data: The app does not store any user data, configurations, or states from within PlugOS on the host. Its design is stateless.

7.3. Security Boundary: It Cannot Threaten PlugOS Even if Compromised

The companion app lies outside PlugOS's trusted boundary; it belongs to the untrusted zone. Even if the host app is maliciously tampered with or fully controlled by a hacker, it cannot decrypt or steal any data within PlugOS. PlugOS's security stems from independent hardware, system encryption, and strict boundaries—not from reliance on the companion app's behavior. This design eliminates trust risks associated with closed-source host apps.

8. Security Organization and Personnel Management

The security of PlugOS comes not only from its technical architecture but also from a robust organizational and management system. We have established dedicated security R&D, testing, compliance, and emergency response teams to form a complete security loop from development to operation.

- **Security R&D and Testing**: Continuously exploring cutting-edge security technologies, combining multi-dimensional testing with penetration verification to ensure that PlugOS's security performance constantly evolves.
- **Compliance and Governance**: We closely adhere to global regulations and industry standards, conducting strict reviews of data processing activities to meet regulations like GDPR and PIPL.
- **Emergency Response**: We have established a rapid response mechanism that covers the prevention, handling, and tracking of security events.
- **Personnel Management**: From recruitment and onboarding to ongoing employment, employees undergo strict background checks, sign confidentiality agreements, are assigned tiered permissions, and receive security training. This ensures that information security responsibilities are assigned to specific individuals.

9. Secure Development Lifecycle Management

PlugOS embeds security and privacy requirements throughout the entire software development process, forming an SDL management system that complies with international standards:

- **Requirements and Design**: Conducting security threat modeling and compliance assessments, putting security metrics first to ensure risks are avoided at the architectural level.
- **Secure Development**: Following international secure coding standards (NIST, ETSI, OWASP, etc.), combining automated tools with manual review to eliminate common vulnerabilities.
- **Security Testing**: Performing multi-level testing and third-party compliance verification, including encryption strength, data protection mechanisms, and penetration testing, to generate professional security reports.
- **Continuous Assurance**: After the product is released, continuously pushing security updates, monitoring for vulnerabilities, and quickly fixing them to ensure PlugOS ensure PlugOS remains secure and controllable throughout its lifecycle.

10. Security Operations and Maintenance

PlugOS's security is reflected not only in its technical architecture and mechanisms but also in its ongoing operational security, compliance adherence, and external certifications, upholding the highest industry security standards. We understand that the foundation of user trust lies not in self-proclamation, but in a verifiable, auditable, and certifiable security operations and maintenance management system.

10.1. Secure Updates and Maintenance

PlugOS has built a secure, transparent, and traceable update mechanism:

- **Signed and Encrypted Update Packages**: All updates are officially signed and distributed via encrypted channel. Before installation, they must pass digital signature verification and integrity checks.
- **Differential Update Mechanism**: While ensuring security, this mechanism reduces the size of update packages, minimizing the impact of updates on the user experience.
- **Quick Rollback Capability**: If an update is found to have compatibility or potential risks, the user can roll back to the previous stable version with one click.
- **Least Privilege Execution**: The update process strictly operates with the least privilege, preventing the update service itself from becoming attack vector.

10.2. Security Emergency Response Center

We believe that open collaboration with the security community is key to improving product security. Therefore, we have established a standardized Product Security Emergency Response Center to provide users with full-lifecycle security response:

- **Security Technical Support**: We provides real-time response and solutions for security issues encountered by Users during use (e.g., data protection after device loss), forming a collaborative loop between product security operations and Users security management.
- **Bug Bounty Program**: We actively encourage and reward security researchers, academics, and white-hat hackers worldwide to conduct security testing on PlugOS. We have launched a bug bounty program that provides cash rewards to individuals and teams who discover and responsibly report valid security vulnerabilities to us.
- **Public Vulnerability Disclosure Policy**: We have formulated and made public a detailed vulnerability disclosure policy, providing a clear and secure channel for the security research community to report vulnerabilities. We are committed to promptly acknowledging and evaluating reports, maintaining communication with the reporter, and publicly thanking them after the vulnerability has been fixed.
- **Cross-Industry Collaboration**: We continuously establish collaboration channels with security vendors, research institutions, and open-source communities to stay updated on threat intelligence and respond promptly.

11. User-Operable Security Verification Checklist

To help users maximize the security capabilities of PlugOS, we recommend that users regularly check the following security verification checklist:

- **Keep Your Product Key Secure**: Users must store their product key securely. If you are concerned about potential leakage of your product key, you can reset it in the PlugOS settings.
- **Check Bound Hosts**: Regularly review the list of bound hosts in the settings and remove any devices that are no longer in use or are untrusted.
- **Minimize Permissions**: Follow the principle of "on-demand," only granting sensitive permissions (e.g., camera, microphone, location) to applications when they are needed.
- **Configure Network Whitelists**: For applications that handle highly sensitive data, use the firewall function to restrict their network access.
- **Enable Anti-Brute Force**: Based on your risk assessment, enable the feature that automatically triggers self-destruction after N incorrect password attempts. Be sure to back up your data beforehand.
- **Set a Duress Password**: To mitigate the risk of potential physical coercion, pre-set a password for decoy mode.
- **Regular Data Backup**: Your data is invaluable and you need back it up regularly to prevent loss.
- **Keep the System Updated**: Install official security updates promptly to ensure the system remains in optimal protective state.

12. Conclusion

PlugOS is more than just a product, it is the practical embodiment of a security philosophy. It provides users with a true digital safe by anchoring the root of trust in independent, verifiable hardware, and combining a multi-layered defense architecture with forward-looking privacy protection design.

With a verifiable hardware chain of trust, independent third-party security certifications, a unique zero-trust architecture, and a data self-destruct mechanism, PlugOS delivers a reliable, robust, and transparent solution for users with the highest demands for data sovereignty and personal privacy. We believe that by returning full control to users, PlugOS is setting a new benchmark for the future of mobile security.