Белая Книга по Безопасности PlugOS

Версия: V1.1

Заявление

Содержание данного документа может обновляться периодически.

Настоящий документ предназначен исключительно в качестве руководства по использованию, и все заявления, информация и рекомендации, содержащиеся в нем, не являются явными или подразумеваемыми гарантиями.

Содержание

1. Предисловие

1.1. Аннотация

В связи с участившимися инцидентами, связанными с безопасностью данных, и ростом глобальной осведомленности о защите конфиденциальности, безопасность мобильных и персональных вычислительных устройств стала одной из ключевых проблем информационного общества. Пользователи опасаются как взломов со стороны хакеров и кражи данных злонамеренными приложениями, так и утечки личной информации в результате принудительной проверки или потери устройства. Традиционные мобильные устройства, такие как смартфоны, зачастую ориентированы на функциональность и коммерческую выгоду, что затрудняет обеспечение суверенитета граждан над своими данными.

PlugOS — это безопасная операционная система, работающая на независимом портативном оборудовании. Ее основные принципы проектирования — приоритет конфиденциальности, модель «нулевого доверия» и минимальные границы доверия — лежат в основе многоуровневой архитектуры защиты, охватывающей аппаратное обеспечение, ядро, систему и приложения.В данном техническом документе раскрываются сведения о соответствии PlugOS стандартам сертификации, модели угроз безопасности, архитектуре безопасности и конфиденциальности, а также управлении безопасностью. Это дает техническим экспертам, специалистам по безопасности, руководителям и всем пользователям, заинтересованным в цифровых правах, прозрачную, проверяемую и поддающуюся аудиту точку зрения, отвечая на самый важный вопрос: почему PlugOS заслуживает обоснованного доверия пользователей.

1.2. Введение

1.2.1. Предпосылки: все более серьезные вызовы в области конфиденциальности и безопасности

В эпоху высокой взаимосвязанности цифровых технологий личные данные превратились из носителей информации в ключевой актив, определяющий бизнес-решения и технологические итерации. От повседневных записей о покупках и данных о местоположении до биометрической информации и данных финансовых счетов — все это несет в себе ключевые права и интересы пользователей.В основных операционных системах широко распространена тенденция к приоритету данных: в погоне за коммерческой выгодой часто по умолчанию включается многомерный сбор данных, при этом с помощью системных прав получаются такие сведения, как время использования приложений и информация об аппаратном обеспечении устройства; более того, даже без явного разрешения пользователя фрагментированные данные объединяются в профиль пользователя, который используется для таргетированной рекламы, рекомендаций продуктов или передачи третьим сторонам.Такая модель пассивного сбора размывает границы конфиденциальности, приводит к потере контроля над цепочкой передачи данных, и часть данных может попадать на зарубежные серверы или в неавторизованные организации. Пользователи не знают, как используются их данные, и им трудно отозвать разрешение, что серьезно ослабляет их право на распоряжение собственными данными.

В то же время суверенитет пользователей над своими данными сталкивается с комплексными угрозами, характеризующимися множественностью сценариев, высокой степенью скрытности и сильной разрушительной силой. На сетевом уровне методы атак на мобильные устройства совершенствуются: хакеры подделывают пакеты обновлений системы, используют уязвимости для внедрения вредоносного кода с целью кражи зашифрованных данных, а фишинговые атаки путем маскировки побуждают пользователей раскрывать конфиденциальную информацию. В 2024 году количество случаев мобильного фишинга в мире увеличилось на 37 % по сравнению с предыдущим годом, причем почти 60 % из них были направлены на ценные данные в сфере финансов и медицины;На физическом уровне часто происходят кражи устройств и целенаправленные атаки; злоумышленники разбирают аппаратное обеспечение для извлечения незашифрованных данных, а уязвимости в цепочке поставок приводят к тому, что устройства подвергаются мониторингу уже при выходе с завода, что затронуло более 10 миллионов конечных устройств.

Кроме того, физическое принуждение и атаки с использованием социальной инженерии становятся скрытой угрозой: пользователи могут под давлением раскрыть пароли разблокировки или биометрические данные, а атаки с использованием социальной инженерии используют психологические слабости для прорыва защитных линий. Переплетение этих угроз приводит к утечке пользовательских данных, материальным убыткам и даже к краже личных данных и нанесению ущерба репутации, что подчеркивает актуальность создания системы с высоким уровнем безопасности и надежной защитой конфиденциальности.

1.2.2. PlugOS: переосмысление цифрового суверенитета

PlugOS был создан именно для решения вышеупомянутых проблем. Это не просто инкрементальное исправление безопасности существующих систем, а переосмысление выходящее из первоочередных принципов, которое привело к созданию вычислительной платформы, основанной на безопасности и конфиденциальности.PlugOS интегрирует полную среду работы интеллектуальной системы, основные приложения и пользовательские данные в одно автономное портативное устройство. Оно взаимодействует с хост-устройством пользователя через зашифрованный канал, обеспечивая ввод-вывод (I/O) с экрана, клавиатуры и сети, создавая тем самым надежную вычислительную среду, поддающуюся проверке и контролю и строго физически изолированную от хост-среды.PlugOS ломает привычку сбора данных, присущую основным операционным системам, и благодаря архитектуре глубокой защиты на всех уровнях — от аппаратного обеспечения до ядра, системы и приложений — внедряет дизайн, ориентированный на конфиденциальность и безопасность, в каждый технический элемент. Это не только защищает от рисков внешних атак, но и гарантирует пользователям право на информированность, контроль и удаление личных данных у их истоков, позволяя операционной системе стать настоящим «хранителем» безопасности пользовательских данных, а не коммерческим транзитным пунктом для их передачи.

1.2.3. Цель белой книги и целевая аудитория

Настоящий технический документ предназначен для технических специалистов, руководителей служб безопасности, лиц, принимающих решения, а также индивидуальных пользователей, уделяющих особое внимание вопросам безопасности и конфиденциальности. В

нем подробно и прозрачно описано, как архитектура и механизмы PlugOS позволяют решать различные задачи безопасности в современном цифровом мире.

Поскольку в данном документе подробно рассматриваются такие специализированные области, как системная безопасность, криптография и аппаратная безопасность, мы предполагаем, что читатель уже обладает определенными базовыми знаниями в области информационной безопасности.

1.3. Термины и определения

В данном документе используются следующие термины и определения.

Термины	Аббревиатуры	Определения
Хост-компьютер/хост-устройство	Host Device	Устройство, которое после подключения PlugOS обеспечивает питание и доступ к периферийным устройствам (таким как экран, клавиатура, сенсорный экран, сеть); это может быть смартфон, планшет или компьютер.
Приложение хост-устройства или клиент хост-устройства	Приложение хоста / сопутствующее приложение	Официальное приложение, установленное на хост-устройстве, являющееся основным мостом взаимодействия PlugOS с хост-устройством. Основные функции включают: перенаправление возможностей периферийных устройств хост-устройства, шифрованную передачу вывода PlugOS, мониторинг состояния и управление.
Ключ продукта	Product Key	Уникальный серийный номер и криптографические учетные данные, записываемые в каждое устройство PlugOS при выпуске, используются для активации устройства и безопасной привязки к хост-компьютеру.
Безопасная привязка	Безопасная привязка	Процесс двусторонней аутентификации при первом сопряжении PlugOS с хост-компьютером, реализующий однозначную привязку устройства к хост-компьютеру посредством проверки пароля и динамического токена, предотвращающий доступ неавторизованных хост-компьютеров.
Доверенная среда выполнения	Trusted Execution Environment (TEE)	Безопасная зона, созданная на вычислительной платформе посредством аппаратной изоляции, которая обеспечивает конфиденциальность и целостность кода и

		данных. TEE используется для выполнения конфиденциальных задач, таких как аутентификация и защита данных, в изолированной среде.
Автономный чип безопасности	Secure Element (SE)	Физически изолированный специализированный микропроцессор с высокой степенью защиты от несанкционированного доступа, предназначенный для хранения и обработки конфиденциальной информации самого высокого уровня (например, шифровальных ключей).
Аппаратный корень доверия	Hardware Root of Trust, HRoT	Основа доверия, созданная еще на этапе производства аппаратного обеспечения и не поддающаяся последующему изменению с помощью программного обеспечения. Она является отправной точкой для безопасного запуска всей системы и операций шифрования.
Архитектура «нулевого доверия»	Архитектура «нулевого доверия»	Модель безопасности, основной принцип которой — «никогда не доверяй, всегда проверяй». Она предусматривает строгую аутентификацию и авторизацию любого запроса на доступ к ресурсам, а также по умолчанию не доверяет хост-машине и ее приложениям.
Поверхность атаки	Attack Surface	Совокупность всех точек входа в систему, которые могут быть использованы злоумышленником для проведения атаки. Чем меньше поверхность атаки, тем, как правило, безопаснее система.
Сквозное шифрование	End-to-End Encryption, E2EE	Схема шифрования связи, обеспечивающая, что данные на протяжении всего процесса передачи от отправителя к получателю остаются зашифрованными, и только участники связи могут их расшифровать.
Отпечаток устройства	Отпечаток устройства	Технология, позволяющая создать «отпечаток», который однозначно идентифицирует устройство, путем сбора различных характеристик его аппаратного и программного обеспечения; часто

		используется для отслеживания пользователей.
Виртуализация датчиков	Виртуализация датчиков	Перехват доступа приложений к аппаратным датчикам на системном уровне и предоставление им виртуальных данных, контролируемых пользователем, с целью противодействия отслеживанию по отпечатку устройства.
Пароль принуждения	Пароль принуждения / Код принуждения	Механизм безопасности, предназначенный для ситуаций физического принуждения; ввод этого пароля приводит к уничтожению данных или переходу в «поддельную систему», не содержащую реальных данных.
Самоуничтожение данных	Самоуничтожение данных	При выполнении заданных условий (например, инициирование пользователем, обнаружение злонамеренной атаки, ситуация принуждения) система автоматически удаляет все конфиденциальные данные (такие как пользовательские файлы, ключи, данные приложений), причем после удаления не остается никаких следов, и восстановление с помощью технических средств невозможно. В условиях самоуничтожения аппаратного обеспечения устройство может перестать функционировать нормально.
Атака на цепочку поставок	Атака на цепочку поставок	Злоумышленник не атакует непосредственно конечного пользователя, а нацеливается на уязвимые места в цепочке поставок — на этапах проектирования, производства, дистрибуции и т. д. — с целью внедрения вредоносного кода.
Уровень гарантии оценки по Общим критериям	Common Criteria, CC EAL	Международный стандарт оценки безопасности ИТ-продуктов; чем выше уровень EAL, тем выше степень гарантии безопасности продукта.
Минимизация данных	Минимизация данных	Один из основных принципов защиты конфиденциальности, требующий, чтобы системы и организации собирали и использовали только минимальный объем личной информации, необходимый для достижения бизнес-целей.

2. Ответственность за безопасность

В процессе реагирования на все более серьезные вызовы в области конфиденциальности и безопасности PlugOS и клиенты должны четко определить свои обязанности в области безопасности, построить систему совместной безопасности, основанную на технических гарантиях и пользовательских нормах, совместно реагировать на многоаспектные вызовы безопасности и совместно защищать суверенитет данных и конфиденциальность.

2.1. Ответственность PlugOS за безопасность

В процессе проектирования и эксплуатации PlugOS несет основную ответственность за техническую и нормативную безопасность, обеспечивая надежность самой системы как «основы безопасности», что конкретно включает:

- **Безопасность технической архитектуры**
  - **Физическая и логическая изоляция**: PlugOS независим от хост-системы, обладает собственными вычислительными и хранилищными ресурсами на аппаратном уровне, что предотвращает смешивание данных с хост-машиной.
  - **Защита на аппаратном уровне**: защита выполнения и ключей с помощью доверенных компонентов, таких как TEE и SE; поддержка высокоуровневого шифрования и хеш-проверки для обеспечения конфиденциальности и целостности.
  - **Защита от принудительных атак**: встроенные механизмы очистки после брутфорс-атак и самоуничтожения паролей под угрозой, предотвращающие утечку данных в результате физического хищения или физического принуждения.
- **Обеспечение защиты данных и конфиденциальности**
  - По умолчанию сбор данных сведен к минимуму: отсутствие рекламы, push-уведомлений и слежения.
  - Локальное хранение и обработка данных, что позволяет избежать скрытой отправки данных и рисков, связанных с трансграничным перемещением данных.
- **Безопасная эксплуатация и соответствие нормативным требованиям**
  - Создание механизмов мониторинга уязвимостей и реагирования на них, внедрение регулярных обновлений и исправлений.
  - Внедрение программы вознаграждений за обнаружение уязвимостей для совместного повышения безопасности с сообществом и партнерами.
  - Обеспечение соответствия системного дизайна международным и национальным стандартам безопасности (например, GDPR, PIPL, ISO/IEC 27001).
- **Поддержка клиентов и реагирование на чрезвычайные ситуации**
  - Предоставление технической поддержки и рекомендаций по вопросам безопасности.

- В случае возникновения чрезвычайных ситуаций (например, утеря оборудования, подозрительное вторжение) мы оперативно помогаем изолировать риски и восстановить безопасность.

2.2. Ответственность клиентов за безопасность

Клиент, как конечный пользователь PlugOS, играет ключевую роль в управлении и использовании оборудования. Осведомленность клиента в вопросах безопасности и соблюдение им правил эксплуатации являются залогом максимальной эффективности системы безопасности. Основные обязанности клиента в области безопасности включают:

- **Надлежащее управление учетными данными и учетными данными устройств**: надлежащее хранение паролей для разблокировки устройств, ключей продукта и других ключевых учетных данных, а также неразглашение учетных данных третьим лицам. Рекомендуется использовать надежные пароли для повышения безопасности учетной записи.
- **Осторожное управление правами доступа и авторизация приложений**: разумно настраивайте системные права в соответствии с фактическими потребностями, не предоставляйте без необходимости третьим сторонам доступ к конфиденциальным данным (таким как местоположение, адресная книга), чтобы с самого начала снизить потенциальный риск атак с использованием социальной инженерии.
- **Внимательность к окружающей среде и соблюдение правил эксплуатации**: при использовании PlugOS для обработки конфиденциальной информации необходимо проявлять высокую бдительность в отношении физического окружения, проверяя, нет ли поблизости скрытых устройств наблюдения (таких как камеры или записывающие устройства). Кроме того, следует избегать выполнения конфиденциальных операций в общественных местах с интенсивным движением людей и высоким риском подглядывания (таких как открытые офисные зоны или общественный транспорт).
- **Обеспечение физической безопасности устройства**: несмотря на то, что PlugOS обладает защитой от несанкционированного доступа на аппаратном уровне, клиентам по-прежнему необходимо бережно хранить само устройство, предотвращая его утерю и не давая злоумышленникам возможности косвенно получить информацию посредством физического контакта или манипуляций.
- **Обеспечение обновления системы и своевременное реагирование**: следите за рассылаемыми PlugOS рекомендациями по безопасности и уведомлениями об обновлениях, своевременно выполняйте обновления системы, чтобы обеспечить постоянную работу устройства на последней безопасной версии. В случае потери устройства, подозрения на утечку данных и других нештатных ситуаций немедленно свяжитесь с технической службой PlugOS, чтобы запустить процедуру реагирования на чрезвычайные ситуации и свести риск распространения угрозы к минимуму.

3. Сертификация безопасности и соответствие нормативным требованиям

В вопросах безопасности и соответствия требованиям PlugOS полагается не только на собственные обязательства, но и на тройную гарантию, состоящую из **«международных авторитетных сертификатов, соответствия глобальным нормам и участия в разработке отраслевых стандартов»**, что позволяет создать стандарты безопасности, которым доверяют даже самые взыскательные пользователи. Мы придерживаемся концепции соответствия «внешняя независимая проверка + постоянное внутреннее совершенствование», чтобы обеспечить долгосрочную надежность PlugOS во всем мире. В этом разделе представлены полученные нами сертификаты, соблюдаемые законы и нормативные акты, а также отраслевые стандарты, в разработке которых мы принимаем участие.

3.1. Сертификация по международным системам

Наши системы исследований и разработок, а также управления строго следуют международным авторитетным стандартам; на каждом этапе — от анализа потребностей и проектирования архитектуры до разработки и тестирования — учитываются строгие требования безопасности. Мы получили множество авторитетных сертификатов от третьих сторон, включая ISO/IEC 9001:2015, ISO/IEC 27001:2022,ISO/IEC 27701:2019, ISO/IEC 29151:2017, CMMI Уровень 3 и т. д. Это в полной мере доказывает, что PlugOS обладает зрелыми, стандартизированными и устойчивыми способностями в области информационной безопасности, защиты конфиденциальности и управления разработкой программного обеспечения, что закладывает прочную основу для превосходных характеристик безопасности PlugOS.

3.1.1. ISO/IEC 9001 (сертификация системы менеджмента качества)

ISO/IEC 9001 — это универсальный международный стандарт системы управления качеством, совместно выпущенный Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC). В его основе лежат три основных принципа: ориентация на клиента, процессуальный подход и постоянное совершенствование. Стандарт предоставляет организациям систематизированную структуру управления качеством, гарантирующую стабильное удовлетворение потребностей клиентов и соответствие нормативным требованиям на протяжении всего жизненного цикла продуктов и услуг.

ISO/IEC 9001 является краеугольным камнем системы управления качеством PlugOS. Благодаря интеграции требований стандарта во все этапы процесса — от разработки и производства до поставки и обслуживания — PlugOS достигает целей стабильности функций безопасности, единообразного пользовательского опыта и эффективного реагирования на

потребности пользователей, предлагая пользователям операционные системы, сочетающие в себе безопасность и высокое качество.

3.1.2. ISO/IEC 27001 (сертификация системы управления информационной безопасностью)

Стандарт системы управления информационной безопасностью (ISO 27001) был разработан совместно Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC) и является авторитетным стандартом в области управления информационной безопасностью, широко признанным во всем мире. ISO 27001 играет незаменимую роль в защите информационных ресурсов и содействии здоровому развитию информатизации, обеспечивая эффективную защиту информационных ресурсов, а также здоровое, упорядоченное и устойчивое развитие процессов информатизации.

ISO 27001 четко определяет требования и передовые практики в области управления информационной безопасностью, обеспечивая рамки безопасности для управления исследованиями и разработками PlugOS. Учитывая информационную безопасность еще на этапе планирования проекта, мы гарантируем соответствие стандартам безопасности на всех этапах, помогая организациям выполнять нормативные требования в области информационной безопасности и избегать правовых рисков и ущерба репутации, связанных с нарушениями.

3.1.3. ISO/IEC 27701 (сертификация системы управления конфиденциальностью информации)

ISO/IEC 27701 — это международный стандарт, разработанный совместно Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC). Он представляет собой расширение стандарта системы управления информационной безопасностью ISO/IEC 27001 и посвящен управлению конфиденциальной информацией. Стандарт предоставляет организациям систематизированную и практическую структуру для защиты персональных данных, а его требования глубоко согласованы с основными глобальными законодательными актами в области конфиденциальности (такими как китайский PIPL, европейский GDPR, американские CCPA/CPRA,LGPD в Бразилии и др.).

На основе ISO/IEC 27701 мы проанализировали процессы управления персональными данными PlugOS на протяжении всего их жизненного цикла, создали стандартизированный механизм предотвращения и контроля рисков в области конфиденциальности, устранили пробелы в управлении и продолжаем оптимизировать систему.

3.1.4. ISO/IEC 29151 (Система управления защитой персональных данных)

ISO/IEC 29151 — это международный стандарт по защите персональных данных, совместно выпущенный Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC). Он фокусируется на кодексах поведения, которым должны следовать обработчики персональных данных при их обработке, и направлен на усиление защиты персональных данных, тем самым защищая права общественности на конфиденциальность и играя важную роль в процессе глобальной цифровизации.

PlugOS строго соблюдает этот стандарт, регламентируя операции по сбору, хранению,

обработке, использованию и раскрытию персональных данных, что позволяет коренным образом защитить право пользователей на неприкосновенность частной жизни.

3.1.5. Сертификация CMMI уровня 3 (сертификация по модели зрелости способностей уровня 3)

CMMI (Capability Maturity Model Integration, интеграция модели зрелости способностей) — это всемирно признанный авторитетный стандарт оценки способностей организации в области управления проектами, инженерной разработки и управления процессами. При этом уровень CMMI 3 (управляемый уровень, Managed Level) является ключевым этапом перехода организации от пассивного реагирования к активному контролю, обозначая, что основные бизнес-процессы организации уже стандартизированы и нормированы и позволяют стабильно обеспечивать высокое качество результатов на основе процессов.

Разработка и проектирование PlugOS на протяжении всего процесса осуществляются с использованием CMMI в качестве основной рамки. В соответствии с требованиями CMMI к стандартизации процессов, нормализации исполнения и повторному использованию активов, концепция управления CMMI внедрена во весь жизненный цикл PlugOS, включая анализ требований, проектирование архитектуры, разработку, тестирование, поставку и эксплуатацию. Это обеспечивает безопасность, стабильность и расширяемость продукта на самом истоке, предоставляя пользователям высоконадежную и безопасную операционную систему с низким уровнем риска.

3.2. Сертификация безопасности продукта

Безопасность PlugOS основана на аппаратных компонентах, прошедших проверку по самым строгим отраслевым стандартам; эти аппаратные компоненты в настоящее время прошли сертификацию по системе CC (Common Criteria). Система сертификации CC (Common Criteria for Information Technology Security Evaluation, Общие критерии оценки безопасности информационных технологий) является на сегодняшний день самым авторитетным и универсальным стандартом оценки продуктов и систем информационной безопасности в мире. Она обеспечивает взаимное признание результатов оценки безопасности между разными странами и регионами, предоставляя предприятиям и организациям надежную основу для выбора продуктов безопасности.

3.2.1. Сертификация безопасности TEE OS

Встроенная в PlugOS ОС TEE, являющаяся ключевой линией защиты безопасности системы, успешно прошла сертификацию безопасности уровня CC EAL 4+, что не только

подтверждает ее способность противостоять обычным атакам, но и демонстрирует ее безопасность и надежность в условиях массового коммерческого использования, являясь важной гарантией нашего технического потенциала и безопасности пользователей.

Кроме того, данная TEE OS прошла проверку в условиях массового производства продуктов в объеме миллиардов единиц. Практика массового производства в таком масштабе не только подтвердила надежность TEE OS на техническом уровне, но и доказала ее применимость и стабильность в условиях крупномасштабного коммерческого использования, благодаря чему пользователи, использующие PlugOS, могут быть полностью уверены в ее безопасности.

3.2.2. Сертификация безопасности SE

Независимый компонент безопасности (SE), используемый в PlugOS, благодаря своим превосходным функциям безопасности создает для пользователей нерушимый барьер безопасности. Этот чип получил сертификат безопасности уровня CC EAL 6+, занимающий высокое положение в глобальной системе стандартов безопасности, что обеспечивает прочную основу безопасности для различных сценариев применения.

Сертификация CC EAL 6+ гарантирует стабильную работу этого чипа в сложной финансовой среде. Будь то использование PlugOS для основных банковских транзакций или защита конфиденциальной информации пользователей, такой как платежные пароли и записи о транзакциях, система обеспечивает надежную защиту, позволяя пользователям без опасений пользоваться цифровыми финансовыми услугами.

3.3. Соответствие мировым законодательным нормам

PlugOS следует принципам «дизайн как **конфиденциальнос**ть» и «минимизация данных»: мы не собираем, не обрабатываем и не храним никаких данных, позволяющих идентифицировать пользователя. Такая архитектура обеспечивает естественное соответствие основным требованиям ведущих мировых законодательных актов о защите данных, таких как «Закон Китайской Народной Республики о защите персональных данных» (PIPL), «Общий регламент по защите данных» (GDPR) ЕС и «Закон штата Калифорния о защите прав потребителей» (CCPA) США.

3.3.1. «Закон Китайской Народной Республики о защите персональных данных» (PIPL)

Закон о защите личных данных (PIPL) — это первый в Китае нормативный акт, разработанный в соответствии с Конституцией с целью защиты прав и интересов в сфере личных данных, регулирования деятельности по обработке личных данных и содействия их рациональному использованию. В законе четко оговорено, что личные данные физических лиц находятся под защитой закона, и ни одна организация или физическое лицо не вправе ущемлять права и интересы физических лиц в отношении их личных данных. Данный закон распространяется на всю деятельность по обработке личных данных физических лиц на территории Китая.

Дизайн и функционал PlugOS полностью соответствуют требованиям данного закона. С точки зрения концепции дизайна PlugOS придерживается принципа «дизайн как

конфиденциальность», категорически отказывается от сбора данных и анализа поведения, система не содержит рекламы, не дает рекомендаций, не ведет прослушивание и не загружает данные, полностью уважает право личности на контроль над собственной информацией и полностью соответствует положениям «Закона Китайской Народной Республики о защите персональных данных», согласно которым обработчики персональных данных должны соблюдать принципы законности, правомерности и добросовестности.

3.3.2. Общий регламент по защите данных (GDPR)

Общий регламент по защите данных (General Data Protection Regulation, сокращенно GDPR) — это чрезвычайно влиятельный нормативный акт Европейского союза в области защиты данных. Этот регламент имеет далеко идущие последствия не только для организаций на территории ЕС, но и для всех предприятий по всему миру, которые занимаются обработкой персональных данных граждан ЕС, — они обязаны адаптировать свои стратегии управления данными для обеспечения соответствия требованиям. GDPR установил стандарты в глобальной сфере защиты данных, в значительной степени изменил подход предприятий к обработке персональных данных и способствовал выходу защиты персональных данных на новый уровень.

PlugOS полностью соответствует строгим требованиям Общего регламента по защите данных (GDPR). Мы придерживаемся концепции «дизайн для конфиденциальности», исключая сбор данных и анализ поведения. Наши независимые безопасные чипы SE или компоненты доверенной исполняемой среды (TEE) обеспечивают шифрование хранения, безопасный запуск и защиту от несанкционированного доступа на аппаратном уровне, гарантируя безопасность и конфиденциальность данных. Механизм самоуничтожения позволяет быстро уничтожить данные, предотвращая утечку, и всесторонне защищая права пользователей на данные.

3.3.3. «Закон о защите прав потребителей штата Калифорния» (CCPA)

«Закон штата Калифорния о защите прав потребителей» (CCPA) — это закон штата Калифорния, принятый для укрепления прав жителей штата на конфиденциальность и защиты потребителей. Являясь первым в США всеобъемлющим законодательным актом о конфиденциальности данных, CCPA призван предоставить жителям Калифорнии более широкие права на контроль над своими личными данными и создать прочную правовую основу для защиты конфиденциальности потребителей и безопасности данных.

В соответствии с тенденциями в области защиты конфиденциальности данных PlugOS строго следует требованиям «Закона о защите прав потребителей штата Калифорния» (CCPA). В своей конструкции система исключает сбор данных и анализ поведения, не содержит рекламы, рекомендаций, не осуществляет прослушивание и не загружает данные, полностью уважая право потребителей на контроль над личной информацией, что соответствует основному духу CCPA, наделяющему потребителей правом на управление.В плане реализации функций TEE и SE играют ключевую роль, что соответствует требованиям CCPA к конфиденциальности информации; для защиты данных используются алгоритмы высокого уровня шифрования и механизмы управления ключами, обеспечивающие конфиденциальность, а для проверки целостности — алгоритмы хеширования, что соответствует требованиям CCPA к качеству информации. Кроме того, система поддерживает такие механизмы, как удаление данных при попытке взлома методом перебора и самоуничтожение паролей при принуждении,

что позволяет активно уничтожать информацию в ситуациях высокого риска, надежно защищая права потребителей на информацию и всесторонне выполняя требования CCPA.

3.4. Разработка стандартов и вклад в развитие отрасли

Мы считаем своим долгом содействовать совершенствованию отраслевых стандартов информационной безопасности и принимаем активное участие в разработке ряда ключевых стандартов и спецификаций в области безопасности. Среди них:

- **Отраслевой стандарт:** «Технические требования к eSIM на основе доверенной исполнительной среды (TEE)» (YD/T 6153-2024).
- **Групповые стандарты:** «Технические спецификации безопасности центрального процессора финансового защищенного чипа» (T/BFIA 007—2021), «Технические требования к информационной безопасности цифровых автомобильных ключей для мобильных интеллектуальных терминалов» (T/TAF 074—2020).

Благодаря активному участию в разработке стандартов мы не только поделились с отраслью нашими техническими знаниями, но и заранее интегрировали эти высокие требования к безопасности в архитектуру PlugOS, что позволило нашим продуктам с самого начала разработки соответствовать ведущим отраслевым стандартам безопасности.

3.5. Независимый аудит безопасности третьей стороной и внутреннее управление соответствием

PlugOS создала двухуровневую систему обеспечения соответствия, состоящую из «внешней независимой проверки + внутреннего постоянного совершенствования»:

- **Внешняя независимая верификация**: мы регулярно привлекаем ведущие в отрасли независимые сторонние организации по безопасности для проведения всесторонних тестов на проникновение и аудита безопасности на уровне исходного кода операционной системы PlugOS, аппаратного дизайна, реализации шифрования и клиентских приложений хост-машин.
- **Внутренний замкнутый цикл обеспечения соответствия**: мы создали профессиональную команду по управлению соответствием, которая динамично отслеживает изменения в глобальных нормах и стандартах и проводит внутренний аудит соответствия по всему процессу не реже одного раза в полгода, чтобы обеспечить тесную взаимосвязь между управлением, разработкой и поставкой и постоянно укреплять эффективность соответствия PlugOS.

4. Модель угроз безопасности и принципы проектирования

Надежная система безопасности начинается с глубокого понимания угроз и четкой философии проектирования. Модель угроз безопасности является основой проектирования безопасности PlugOS. Она четко определяет основную сферу защиты, устанавливая, «что защищать», «от кого защищаться», «где проходят границы доверия» и «что невозможно решить».

4.1. Основные защищаемые активы

PlugOS разработана для защиты данных и приложений, хранящихся или работающих внутри PlugOS. К этим активам относятся, помимо прочего:

- **Ключи и учетные данные:** ключи шифрования, токены аутентификации, пароли к различным учетным записям и т. д.
- **Данные о конфиденциальности пользователей:** файлы, записи сообщений, адресная книга, календарь, фотографии, аудио- и видеофайлы и т. д.
- **Метаданные и контент коммуникаций:** сами действия по обмену сообщениями, содержание сеансов, графы взаимосвязей и т. д.
- **Финансовые активы и удостоверения личности:** закрытые ключи цифровых валют, учетные данные для интернет-банкинга, цифровые удостоверения личности и т. д.
- **Местоположение и траектории поведения:** географическая информация, записи об использовании приложений, история сетевых запросов и т. д.

4.2. Основные объекты защиты (модель злоумышленников)

Модель защиты PlugOS охватывает многомерные и многоуровневые типы злоумышленников, включая, помимо прочего, следующие распространенные типы:

- Лица, **применяющие физическое давление**: лица, пытающиеся заставить пользователя разблокировать устройство или передать учетные данные в условиях физического давления или угрозы физической неприкосновенности. Например, в случае похищения на улице прямое сопротивление пользователя может поставить под угрозу его жизнь, а покорность означает двойное ограбление со стороны злоумышленника — как финансовое, так и в плане конфиденциальности.
- **Физические злоумышленники:** технические специалисты, которые после потери или кражи устройства пытаются извлечь данные из него с помощью физических методов, таких как атака холодного запуска (Cold Boot Attack), отладка JTAG, считывание данных путем отпайки чипа (Chip-off Forensics). После кражи устройства злоумышленник пытается извлечь внутренние данные PlugOS с помощью холодного запуска, отпайки чипа и т. д.
- **Злоумышленники** в **цепочке поставок:** внутренние или внешние лица, пытающиеся внедрить аппаратные бэкдоры, вредоносную прошивку или зараженные программные пакеты на этапах производства, транспортировки, распространения или обновления программного обеспечения устройства.
- **Злоумышленники, взломавшие хост-устройство:** злоумышленники, полностью контролирующие хост-устройство (ПК или мобильный телефон), к которому подключена PlugOS, и пытающиеся атаковать PlugOS с помощью вредоносного ПО на стороне хост-устройства.
- **Поставщики вредоносных приложений:** злоумышленники, которые побуждают пользователей устанавливать вредоносные приложения внутри PlugOS с целью кражи данных других приложений, выполнения несанкционированных действий или создания скрытых каналов связи.

- **Сетевой злоумышленник:** злоумышленник, пытающийся прослушивать или подделывать сетевую коммуникацию PlugOS с помощью атак «человек посередине» (MITM), DNS-угона, вредоносных точек доступа Wi-Fi и т. д.

4.3. Граница доверия (нулевое доверие)

Основной концепцией безопасности PlugOS является «нулевое доверие», то есть по умолчанию не доверяется ни одной сети, внешнему приложению и соседним системам. Граница доверия явно и минимально разграничена, чтобы уменьшить уязвимость системы.

- **Доверительная зона (Trusted Zone):** аппаратное оборудование PlugOS и его прошивка, а также операционная система PlugOS с проверенной подписью. Все пользовательские данные и приложения работают в этой зоне.
- **Недоверительная зона (Untrusted Zone):** операционная система хост-машины, клиентские приложения хост-машины, все внешние сети и т. д.

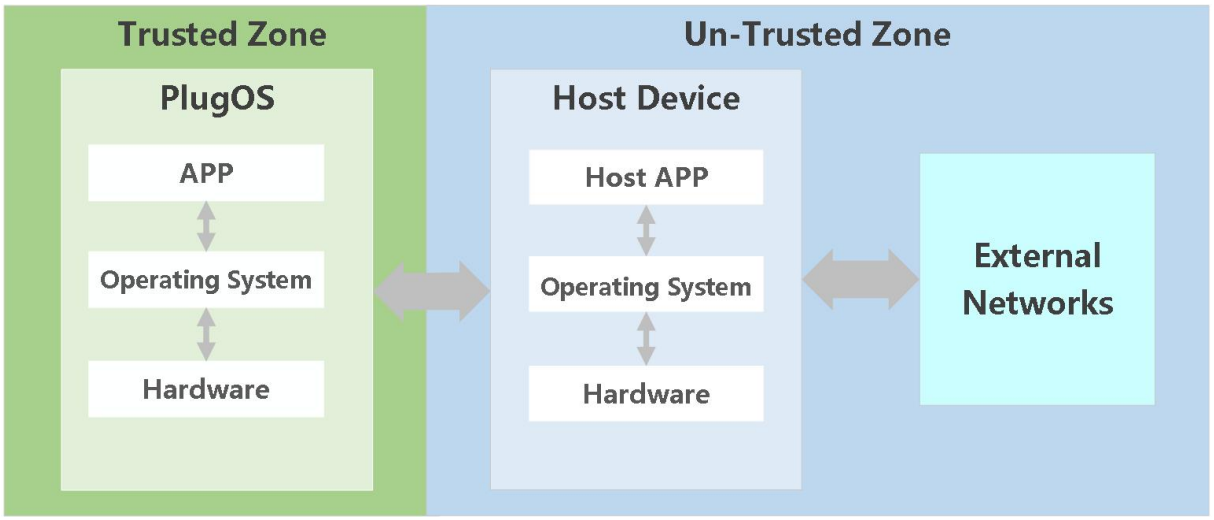


Схема зон границ доверия

Между доверенной и недоверенной зонами существует четкая граница безопасности, обеспечиваемая на аппаратном уровне. Взаимодействие между ними ограничено одним каналом ввода-вывода с сквозным шифрованием. В таблице ниже четко определены обязанности и полномочия обеих зон:

Аспект	Доверительная зона (PlugOS)	Недоверительная зона (хост-машина)
Среда выполнения	Независимое аппаратное обеспечение + доверенная исполнительная среда (TEE/SE) + безопасная операционная система	Открытая система хост-машины (например, Android/iOS/Windows)
Область доступа	Управление всеми внутренними приложениями и данными, наличие возможностей шифрования и изоляции на аппаратном уровне	Выступает исключительно в качестве прокси ввода-вывода, не имеет доступа к каким-либо открытым данным внутри PlugOS
Хранение	Хранение пользовательских данных с	Хранение только

данных	аппаратным шифрованием; данные циркулируют по внутреннему замкнутому контуру	неконфиденциальных настроек, без сохранения пользовательских данных
Ответственность за безопасность	Несет ответственность за безопасность и защиту конфиденциальности пользовательских данных на всем пути от хранения и обработки до уничтожения	Обеспечивает только целостность собственного кода и безопасность каналов связи, не участвует в принятии ключевых решений по безопасности

4.4. Неустранимые угрозы безопасности

В целях обеспечения прозрачности мы обязаны четко указать на те риски безопасности, которые не могут быть напрямую покрыты моделью угроз PlugOS. Эти риски в основном связаны с факторами, находящимися за пределами доверенной зоны, и меры по их снижению зависят от уровня осведомленности и поведения пользователей. В основном они делятся на две категории:

4.4.1. Риски, связанные с ошибками пользователей

PlugOS предназначен для предотвращения несанкционированного доступа, но не может предотвратить небезопасные действия, совершаемые пользователем сознательно или под влиянием обмана. К ним относятся:

- **Социальная инженерия и фишинговые атаки**: пользователя побуждают перейти по вредоносной ссылке, загрузить вредоносное вложение или самостоятельно ввести учетные данные на поддельном веб-сайте.
- **Утечка учетных данных**: пользователь добровольно сообщает другим лицам учетные данные с высоким уровнем доступа, такие как пароль разблокировки или ключ продукта, либо записывает их в небезопасном месте, что приводит к их утечке.
- **Предоставление прав вредоносным приложениям**: пользователи самостоятельно устанавливают в PlugOS приложения неизвестного происхождения и предоставляют им чрезмерные права.

Меры по снижению рисков: PlugOS обеспечивает техническую защиту с помощью таких механизмов, как минимизация прав доступа, изоляция приложений и сетевой брандмауэр, однако последней линией защиты остается осведомленность пользователя в вопросах безопасности. Мы настоятельно рекомендуем пользователям устанавливать приложения только из надежных источников и с осторожностью предоставлять им права доступа. Подробнее см. в главе 11 «Контрольный список мер безопасности, доступных пользователю».

4.4.2. Риски, связанные с недоверенной средой (хост-компьютер и физическая среда)

Границы безопасности PlugOS заканчиваются на его физическом оборудовании. Когда внешняя физическая среда или среда подключенного хост-компьютера полностью

контролируются злоумышленником, существует риск утечки информации.

- **Прослушивание физической среды**: злоумышленник может с помощью внешних скрытых камер, подглядывания и других средств похитить информацию, когда пользователь вводит пароль или смотрит на экран. Это выходит за рамки возможностей защиты любого конечного устройства. Рекомендуется пользователям обеспечивать безопасность физической среды при работе с конфиденциальной информацией.
- **Полностью скомпрометированный хост**: Конструкция PlugOS гарантирует, что даже в случае заражения хоста вредоносным ПО прямой доступ к его внутренним данным в состоянии покоя (Data-at-Rest) и данным во время работы (Data-in-Use) невозможен.Однако данные при отображении (Data-in-Display) и вводе (Data-in-Input) должны проходить через I/O-прокси на недоверенном хост-компьютере. Таким образом, хост-компьютер, полностью контролируемый вредоносным ПО на уровне ядра (например, продвинутым кейлоггером или низкоуровневым инструментом для создания снимков экрана), теоретически может записывать ввод с клавиатуры пользователя и отображаемое на экране содержимое.

Меры по снижению рисков: это архитектурный выбор, представляющий собой компромисс между безопасностью, портативностью и стоимостью.Клиентское приложение PlugOS для хост-устройства имеет встроенные средства проверки безопасности среды выполнения, которые эффективно противостоят большинству атак на уровне приложений, таких как скриншоты, запись экрана и инъекции. Однако ни одна защита на уровне приложений не может дать абсолютной гарантии против атак, исходящих из ядра операционной системы хост-устройства. Поэтому мы рекомендуем пользователям подключать PlugOS к хост-устройствам, над которыми они имеют полный контроль и которые находятся в хорошем состоянии с точки зрения безопасности, чтобы свести этот риск к минимуму.

5. Архитектура безопасности

Архитектура безопасности PlugOS следует основной идее многоуровневой защиты, опираясь на неизменяемый аппаратный корень доверия в качестве фундамента. Благодаря многоуровневым и взаимосвязанным механизмам безопасности создана надежная вычислительная среда, охватывающая весь путь от чипа до приложения.Мы не только используем и усиливаем проверенную модель безопасности AOSP (Android Open Source Project), но и, благодаря архитектурным инновациям, стремимся противостоять крайним угрозам — от физического вторжения и атак на цепочку поставок до принудительного давления — чтобы обеспечить конфиденциальность и целостность пользовательских данных.

В этом разделе мы поочередно проанализируем основные механизмы безопасности PlugOS, начиная с аппаратного обеспечения, чипа, ядра системы, данных и основных сервисов. Цель разработки этих механизмов — обеспечить проверяемую безопасность, основанную на архитектуре, а не на доверии, основанном на обещаниях.

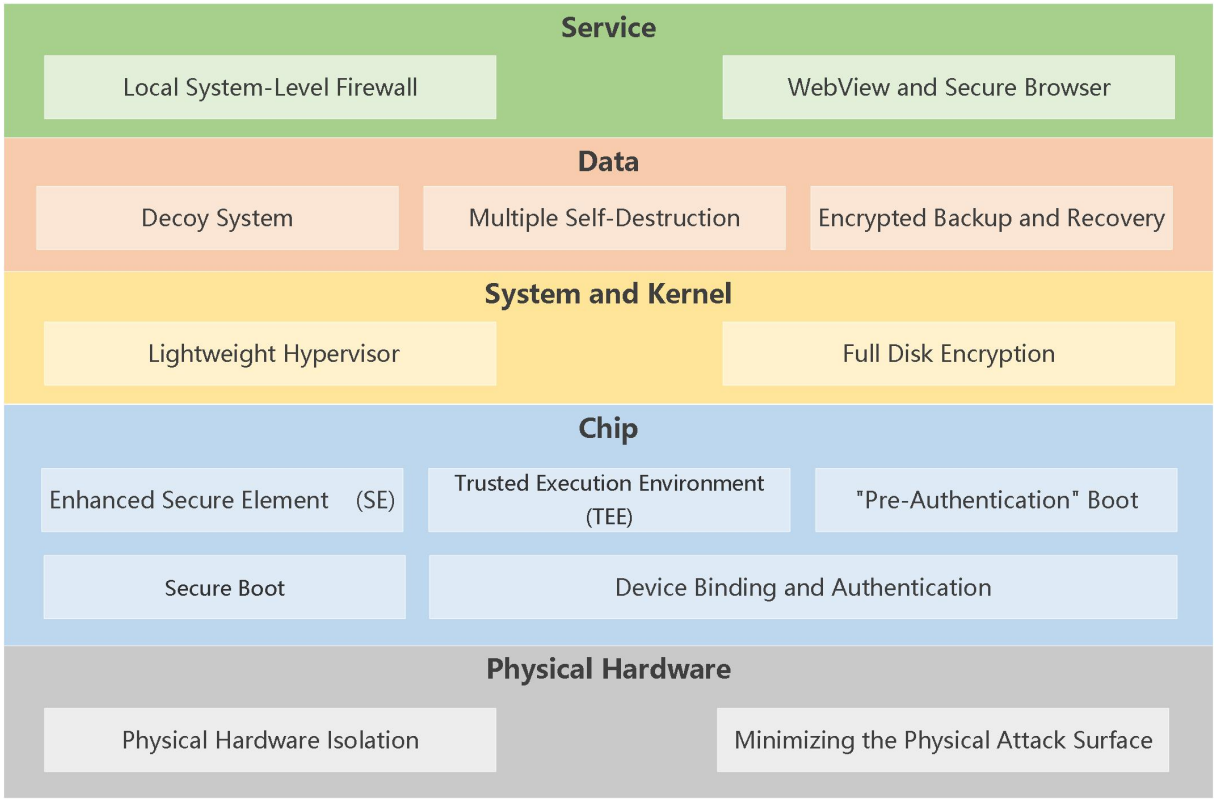


Схема архитектуры безопасности PlugOS

5.1. Физическая изоляция аппаратного обеспечения и минимизация поверхности атаки

Это первая линия защиты от внешних угроз, а также самая наглядная.

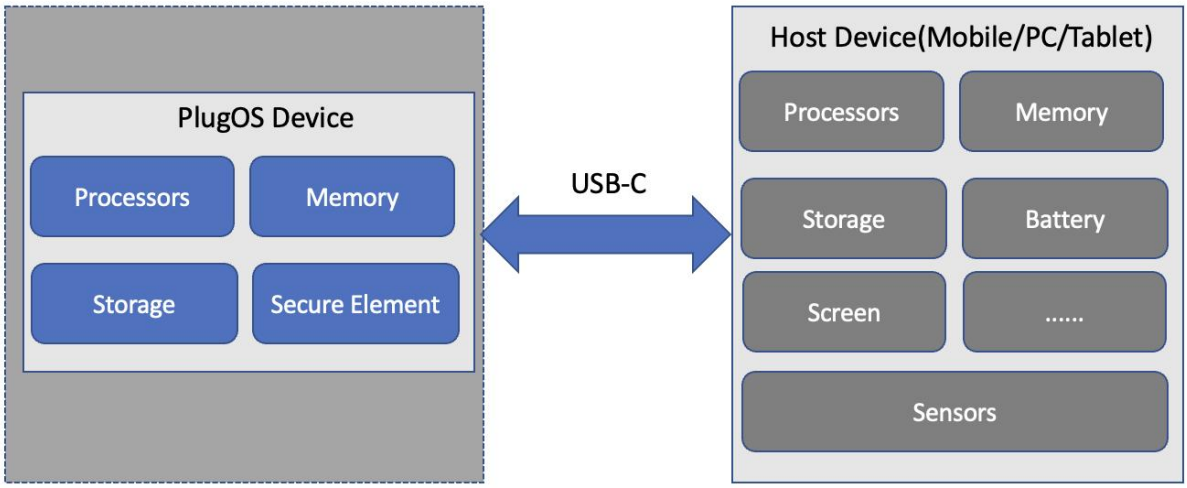


Схема архитектуры аппаратных компонентов

Физическая изоляция аппаратного обеспечения: PlugOS, являясь полнофункциональным автономным вычислительным и хранилищным модулем, оснащен собственным высокопроизводительным процессором, высокоскоростной памятью и хранилищем большого объема и полностью физически изолирован от хост-системы (компьютера или мобильного телефона пользователя). Это означает, что операционная система

хост-устройства (компьютера или мобильного телефона пользователя и т. д.) архитектурно не имеет доступа к адресному пространству памяти или чипам хранения PlugOS. Даже если хост-устройство полностью контролируется вредоносным ПО, оно не сможет преодолеть эту физическую границу.

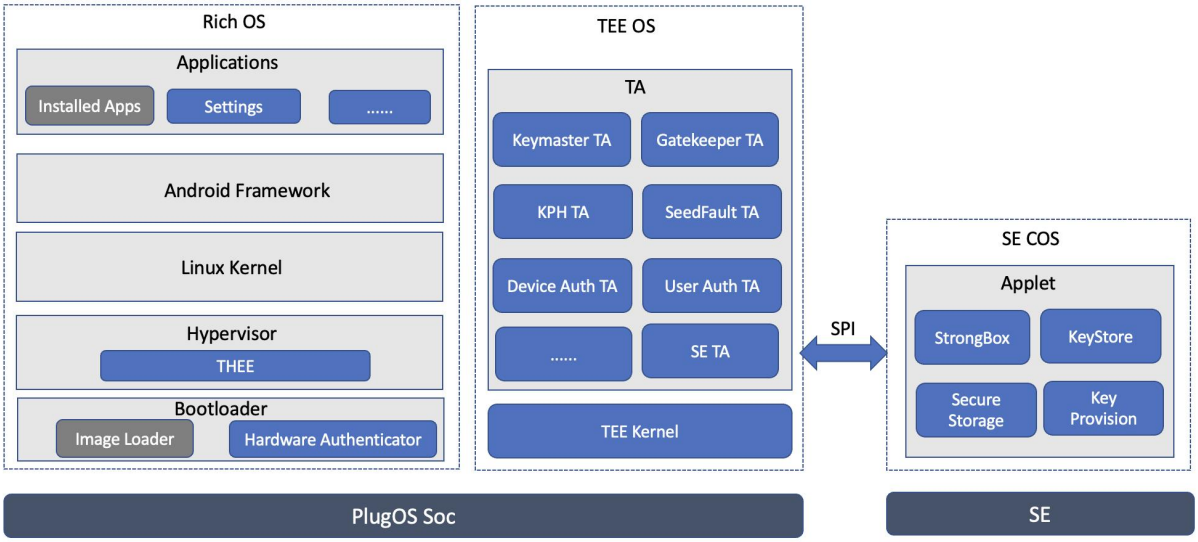
Минимизация физической поверхности атаки: аппаратная конструкция PlugOS следует принципу минимализма. Устройство не содержит сложных радиочастотных компонентов, таких как сотовый модем, NFC, GPS, или ненужных датчиков, и взаимодействует с внешним миром только через один интерфейс USB-C, защищенный протоколом с сильным шифрованием. Такая конструкция значительно сужает физическую и программную поверхности атаки, снижая риск удаленных или ближних атак у истоков.

5.2. Безопасная изоляция на уровне чипа

Аппаратное обеспечение является отправной точкой для любой системы безопасности. Модель безопасности PlugOS начинается с корня доверия, который обеспечивается аппаратно и не может быть подделан программным обеспечением.

5.2.1. Платформа безопасной изоляции на уровне чипа

Основа безопасной изоляции PlugOS основана на защищенном чипе SE и доверенной исполняемой среде TEE, что гарантирует невозможность подделки критически важных операций.



Архитектура чиповой изоляции PlugOS

Усиленный чип безопасности (SE): некоторые модели устройств PlugOS оснащены встроенным независимым чипом безопасности SE, сертифицированным по стандарту CC EAL6+. SE представляет собой миниатюрный безопасный компьютер, защищенный от физического взлома, который обеспечивает защиту ключей шифрования и другой конфиденциальной информации на уровне физического сейфа;CC EAL6+ — один из самых высоких уровней сертификации безопасности чипов на сегодняшний день. PlugOS глубоко интегрирует возможности чипа безопасности и изначально поддерживает спецификацию Android StrongBox Keymaster, гарантируя, что генерация, хранение и использование ключей

полностью осуществляются внутри аппаратного обеспечения, недоступного для любого внешнего программного обеспечения, включая операционную систему, что обеспечивает аппаратную защиту операций шифрования и управления учетными данными на уровне чипа банковской карты.

Доверенная исполнительная среда (TEE): все устройства PlugOS оснащены TEE на базе технологии ARM TrustZone, ядро TEE OS которой предоставляется ведущим в отрасли TrustKernel, прошло сертификацию безопасности CC EAL4+ и проверено в массовом производстве миллиардов устройств.TEE создает для PlugOS параллельную основной операционной системе и аппаратную изолированную среду выполнения для таких ключевых операций безопасности, как двухфакторная аутентификация пользователей и устройств, шифрование и дешифрование данных, управление ключами и управление SE, что эффективно предотвращает влияние уязвимостей основной операционной системы на ключевые функции безопасности.

5.2.2. Архитектурные инновации: процесс запуска с «предварительной аутентификацией»

PlugOS перевернул традиционную модель «аутентификации после запуска». Традиционный безопасный запуск (Secure Boot), хотя и позволяет проверить целостность системной подписи, не может предотвратить выполнение прошивки с встроенным бэкдором до аутентификации пользователя. Например, в настоящее время многие коммерческие программы для взлома могут взламывать и извлекать пользовательские данные с устройства на физическом уровне без авторизации пользователя, в основном используя уязвимости в базовой прошивке устройства.PlugOS решает эту проблему на архитектурном уровне: прежде чем какой-либо системный код будет загружен, проверен и выполнен, устройство должно пройти двойную аутентификацию на уровне чипа — как пользователя, так и самого устройства**. Этот подход исключает возможность обхода системы аутентификации с помощью традиционных методов, таких как физические атаки, заражение цепочки поставок или уязвимости в базовом прошивке.**Например, даже если в прошивке чипа или на уровне ядра Linux присутствуют бэкдоры, пока не будет выполнена двойная аутентификация пользователя и устройства с помощью аппаратного модуля безопасности, прошивка из цепочки поставок, содержащая бэкдоры, никогда не сможет включиться и запуститься.

Безопасный запуск: каждый этап запуска устройства проходит проверку цифровой подписи, формируя полную «цепочку доверия». Любая неавторизованная прошивка или поддельный образ системы не имеет возможности быть загруженной и выполненной, поскольку ключи для расшифровки диска, от которых они зависят, отсутствуют в памяти до успешного завершения аутентификации.

Привязка и аутентификация устройства: PlugOS разрешает подключение только к авторизованным и сертифицированным хост-устройствам. При первом использовании на хост-устройстве пользователю необходимо выполнить привязку к хосту с помощью продуктового ключа устройства PlugOS. При последующих подключениях распознаются только привязанные и прошедшие проверку хост-устройства.Аутентификация хост-устройства основана на распознавании физических характеристик его аппаратного обеспечения. После первоначальной

привязки PlugOS генерирует для хост-устройства пару ключей привязки, которые служат фактором аутентификации при последующих подключениях. В дальнейшем только прошедшие аутентификацию хост-устройства могут вступать с ним в связь, что предотвращает атаки «человек посередине» и несанкционированный доступ.

5.3. Усиление безопасности на уровне системы и ядра

На основе аппаратных гарантий PlugOS создает мощную линию защиты с помощью передовых технологий виртуализации и механизмов обязательного шифрования.

Изоляция ядра на основе легкого гипервизора: в традиционной архитектуре макроядра, как только злоумышленник получает права Root, вся система полностью теряет защиту. PlugOS имеет встроенный собственный легкий гипервизор (виртуальный монитор), который виртуально изолирует ключевые компоненты ядра операционной системы (такие как компоненты управления памятью и компоненты управления политиками безопасности), создавая для каждого приложения независимую зону безопасности, строго ограниченную политиками.Такая конструкция делает практически невозможным горизонтальное распространение уязвимости даже в случае наличия уязвимости в отдельном приложении или системной службе, что ограничивает зону воздействия уязвимости на ядро или другие приложения и повышает защищенность системы от проникновения.

Шифрование всего диска (шифрование при записи): PlugOS по умолчанию использует архитектуру шифрования всего диска на уровне файлов. Любые данные, записываемые на носитель, автоматически шифруются аппаратным шифровальным движком в момент записи.Каждый файл шифруется с использованием отдельного ключа, а эти файловые ключи, в свою очередь, защищены одним главным ключом. Этот главный ключ надежно хранится в TEE/SE и жестко привязан к учетным данным пользователя для разблокировки. Это означает, что даже если злоумышленник с помощью физических средств (например, отпаивания чипа) получит доступ к чипу флэш-памяти, он не сможет прочитать никакой ценной информации в открытом виде.

5.4. Самоуничтожение данных и безопасное восстановление

Помимо надежной традиционной архитектуры безопасности, PlugOS также инновационно внедрил механизмы защиты данных от экстремальных сценариев, таких как физическое воздействие и взлом методом перебора. Это последняя линия защиты безопасности пользовательских данных, которая гарантирует пользователю абсолютный контроль над своими данными.

Для противодействия экстремальным ситуациям принуждения или физического взлома в PlugOS встроены различные механизмы самоуничтожения данных. Этот механизм может быть запущен в результате нескольких последовательных ошибочных вводов пароля или при активном вводе пользователем заранее установленного пароля принуждения на экране разблокировки. После запуска система необратимо уничтожит ключи шифрования, что приведет к необратимому уничтожению всех данных на диске.Одновременно PlugOS предоставляет решение для резервного копирования и восстановления с сквозным шифрованием. Пользователи могут регулярно создавать безопасные резервные копии данных в

выбранном ими надежном хранилище, при этом ключи шифрования находятся под их полным контролем. Это обеспечивает самостоятельное хранение и восстановление данных, гарантируя, что суверенитет над данными всегда остается в руках пользователя.

5.4.1. Пароль принудительной блокировки

- **Принцип работы:** пользователь может заранее установить пароль принудительной разблокировки. При разблокировке с помощью этого пароля PlugOS незаметно удаляет все внутренние данные.
- **Сценарий применения:** в случае принудительного требования разблокировать устройство пользователь может ввести пароль принуждения, чтобы защитить себя и свои данные, превратив устройство в бесполезную цель для злоумышленника.

5.4.2. Механизм самоуничтожения

- **Условия срабатывания:**
  - Защита от брутфорса: количество последовательных вводов неверного пароля достигло установленного пользователем порога.
  - Защита от физического вскрытия (поддерживается только некоторыми моделями): обнаружение несанкционированного вскрытия корпуса устройства или физического воздействия на ключевые микросхемы.
  - Срабатывание по коду принуждения: пользователь может настроить определенный код принуждения для запуска бесшумного самоуничтожения.
- **Процесс выполнения**: при срабатывании TEE или SE запускает необратимую процедуру уничтожения шифровальных ключей, в результате чего данные, зашифрованные на всем диске, мгновенно превращаются в невосстановимый набор символов, что позволяет полностью удалить все конфиденциальные данные.

5.4.3. Шифрованное резервное копирование и восстановление

PlugOS предоставляет возможность сквозного шифрования при резервном копировании и восстановлении, что гарантирует постоянное шифрование всех ваших данных во время резервного копирования, передачи и восстановления, максимально предотвращая несанкционированный доступ. Данные резервной копии подвергаются сквозному шифрованию на устройстве с использованием ключа, известного только пользователю, и только после этого экспортируются в выбранное пользователем место хранения (например, на персональный компьютер, внешнее устройство хранения и т. д.). Процесс восстановления также требует предоставления ключа пользователем для расшифровки на локальном устройстве.Как поставщик услуг, мы не имеем доступа к какому-либо открытому тексту резервных копий пользователей на протяжении всего процесса, что гарантирует полную суверенность пользователей над своими данными во время резервного копирования и восстановления.

5.5. Усиление безопасности ключевых сервисов

PlugOS провел глубокую реорганизацию и укрепление нескольких ключевых системных сервисов, тесно связанных с конфиденциальностью и безопасностью. Например:

Локальный системный брандмауэр: брандмауэр, являясь одним из ключевых

компонентов сетевой безопасности PlugOS, глубоко интегрирован с сетевым стеком системы, что позволяет ему осуществлять жесткий контроль доступа к сетевой активности всех приложений (включая системные). Он работает локально, не передает и не загружает никаких журналов, а также способен распознавать и блокировать встроенные в приложения трекеры (Tracker) и телеметрические соединения (Telemetry).Пользователи могут разрабатывать точные политики сетевого доступа на основе таких параметров, как приложения, доменные имена, IP-адреса и порты, что позволяет обеспечить полный контроль над всеми подключениями.

WebView и безопасный браузер: встроенный браузер PlugOS и компонент WebView в приложениях основаны на Chromium и интегрированы с набором усовершенствованных патчей от ведущих проектов по безопасности.Мы удалили все зависимости от сервисов Google и код телеметрии, по умолчанию отключили высокорисковые веб-API, включили строгую политику изоляции файлов cookie и защиты от отслеживания, а также усилили JIT-компилятор для защиты от атак на память. Это предоставляет пользователям чистую среду просмотра, в которой не осуществляется сбор данных, отслеживание и не происходит никаких помех.

6. Архитектура конфиденциальности

В отличие от моделей основных операционных систем, предполагающих сбор данных и поведения пользователей по умолчанию с возможностью отказа, PlugOS строго следует основному принципу **«конфиденциальность по дизайну» (Privacy by Design)**.Мы никогда не создаем более безопасные рекламные платформы, а на уровне архитектуры искореняем любые формы ненужного сбора данных. Все механизмы PlugOS построены вокруг трех основных целей: **«локализация данных, отсутствие анализа поведения и полный контроль со стороны** пользователя», что гарантирует, что каждое цифровое действие пользователя служит исключительно его собственным намерениям.

В этом разделе подробно описаны основные технологии конфиденциальности, разработанные PlugOS для достижения этих целей.

6.1. Нулевой сбор данных

В традиционных мобильных операционных системах, даже если пользователь отключил большинство опций обмена данными, на системном уровне по-прежнему происходит фоновый телеметрический сбор данных и анализ поведения. Этот незаметный сбор данных часто используется для оптимизации сервисов или таргетированной рекламы, но по сути ослабляет суверенитет пользователя в вопросах конфиденциальности.

Нулевой телеметрический сбор и локализация данных являются краеугольным камнем обязательств PlugOS в области конфиденциальности: **мы не собираем ваши данные, поскольку наша система изначально не имеет такой функции.**

- **Телеметрия и аналитика отключены по умолчанию:** PlugOS построен на базе AOSP, но в процессе компиляции и настройки мы систематически удаляем или отключаем по умолчанию все компоненты сбора данных — от нижнего уровня системы и уровня фреймворка до уровня основных приложений — включая все сервисы Google, а также встроенные в AOSP компоненты сбора данных, такие как телеметрия (Telemetry), отчеты о сбоях и анализ поведения пользователей.В PlugOS отсутствуют какие-либо фоновые

службы, которые отправляют информацию о ваших привычках использования приложений, данных о производительности системы или личных предпочтениях производителю устройства или разработчику программного обеспечения.

- **Без рекламы и рекомендаций:** поскольку не проводится профилирование пользователей и анализ их поведения, система PlugOS в целом не содержит никакой рекламы или персонализированных рекомендаций. Цифровой опыт пользователя определяется его собственной волей, а не алгоритмами.
- **Принципы локализации и минимизации данных**: Наша философия заключается в том, что данные, которые не хранятся, являются самыми безопасными. Мы перепроектировали саму систему и все встроенные базовые приложения (такие как браузер, клавиатура, файловый менеджер), строго следуя принципам локализации и минимизации данных. Например, наша клавиатура обрабатывает ввод пользователя только на локальном устройстве, не осуществляя никакой облачной автозаполнения или загрузки пользовательского словаря.
- **Режим «нулевого знания»:** даже производитель системы TrustKernel не может получить через PlugOS какие-либо конфиденциальные данные пользователя. Вся информация пользователя находится в его руках, а роль производителя ограничивается предоставлением инструментов безопасности.

В традиционных системах, таких как Android/iOS, даже при включенном ограничении отслеживания рекламы система по-прежнему загружает часть анонимизированных данных посредством телеметрии; в PlugOS нет переключателя ограничения, поскольку сбор данных отсутствует с самого начала.

6.2. Виртуализация датчиков: блокировка отслеживания по отпечаткам оборудования

Современные приложения широко используют отпечатки устройств (Device Fingerprinting) для идентификации и отслеживания пользователей. Такие отпечатки обычно создают уникальный идентификатор пользователя и устройства на основе сотен параметров, включая аппаратные характеристики (например, IMEI, ID датчиков, информацию о базовой полосе), сетевую среду (IP, DNS, часовой пояс) и состояние программного обеспечения. Даже если пользователь сменит учетную запись или очистит кэш, ему трудно избежать повторной идентификации и постоянного отслеживания.Определение отпечатков устройства обычно не требует специальных разрешений, незаметно для пользователя и приводит к постоянной утечке личной информации и отслеживанию поведения.

PlugOS, используя технологию виртуализации датчиков на системном уровне, прерывает путь формирования отпечатков устройств, тем самым эффективно защищая личную идентичность и конфиденциальность действий.

6.2.1. Виртуализация идентификаторов

В отношении тех аппаратных идентификаторов, которые могут использоваться в качестве уникальных идентификаторов, PlugOS осуществляет виртуализацию. При запросе такой информации приложениям система выборочно предоставляет общие, бессмысленные значения

по умолчанию или разные случайные значения для разных приложений вместо реальных серийных номеров оборудования, информации о SIM-картах (IMSI/ICCID), MAC-адресов и т. д.

6.2.2. Моделирование данных датчиков

Пользователь может с помощью централизованной панели управления конфиденциальностью моделировать различные виды информации об окружающей среде по мере необходимости, предоставляя приложениям ложные, но правдоподобные данные для удовлетворения их рабочих потребностей, одновременно защищая реальную информацию. Например:

- **Виртуальное географическое положение**: пользователь может установить фиксированное виртуальное местоположение или динамический виртуальный маршрут перемещения.
- **Виртуальное состояние сети**: имитация различных операторов сотовой связи, типов сетей и информации о базовых станциях.

6.2.3. Динамическое переключение прямого доступа к аппаратному обеспечению

При необходимости пользователь может, подтвердив свои полномочия, предоставить прямой доступ к реальному оборудованию хост-компьютера (камера, микрофон, Bluetooth) определенному приложению в PlugOS, гибко переключаясь между доступностью функций и защитой конфиденциальности. Пользователь может в любой момент отозвать разрешение, гарантируя, что доступ к оборудованию открывается только по мере необходимости и закрывается сразу после использования.

Такая конструкция гарантирует, что даже самым агрессивным алгоритмам отслеживания по отпечаткам пальцев будет сложно установить надежную связь с личностью, что максимально защищает анонимность и обезличивание пользователя и устройства.

6.3. Прозрачное и контролируемое сетевое соединение

Сетевой трафик является основным каналом утечки данных. Многие приложения загружают журналы, данные SDK или информацию о поведении на сторонние серверы без уведомления пользователя.

PlugOS имеет встроенный брандмауэр системного уровня, который предоставляет пользователям беспрецедентную возможность отслеживать и контролировать сетевой трафик, позволяя им быть в курсе каждого подключения, контролировать его и отслеживать. Его основным инструментом является брандмауэр на уровне ядра, упомянутый в третьей главе; в этом разделе основное внимание уделяется его функциям защиты конфиденциальности.

- **Распознавание и блокировка трекеров:** встроенная база данных позволяет обнаруживать распространенные рекламные и аналитические SDK в приложениях и предупреждать пользователя о потенциальных рисках для конфиденциальности, связанных с данным подключением. Пользователь может выбрать блокировку этих сторонних трекеров.
- **Аудит подключений:** брандмауэр в режиме реального времени регистрирует все

запросы на сетевые подключения от приложений в системе и представляет их пользователю в понятной и наглядной форме, включая целевые домены, IP-адреса и протоколы. Это позволяет избежать скрытой отправки данных и выявить все попытки передачи данных, скрывающиеся за приложениями. Пользователь может заблокировать сетевые подключения определенных приложений или целевых серверов.

- **Режим «белого списка»:** для сценариев, связанных с обработкой особо конфиденциальных данных, пользователь может включить строгий режим «белого списка», при котором по умолчанию запрещены все сетевые подключения, а разрешен доступ только к определенным доменам или IP-адресам, вручную одобренным пользователем. Для сценариев, где подключение к сети совершенно не требуется, пользователь может одним нажатием полностью отключить все сетевые права приложения, исключив возможность утечки информации любым способом.

7. Клиентское приложение хост-машины

Клиентское приложение для хост-компьютера — это сопутствующее приложение PlugOS для мобильных устройств или компьютеров, основная функция которого заключается в том, чтобы помочь PlugOS обращаться к периферийным устройствам хост-компьютера, таким как экран и клавиатура, для обеспечения взаимодействия и отображения информации. В этом разделе будет разъяснено с трех точек зрения — позиционирования, функций и границ — что данное приложение не станет источником угрозы безопасности для PlugOS.

7.1. Основная позиция: ограниченный «прокси ввода-вывода»

Приложение-клиент хост-компьютера разработано в строгом соответствии с принципами минимальных привилегий и нулевого доверия. В модели безопасности PlugOS оно четко отнесено к «недоверенной зоне» (см. раздел 4.3), а его основная роль заключается в том, чтобы выступать в качестве «прокси ввода-вывода (I/O Proxy)» с ограниченными функциями, служа мостом между пользователем и аппаратными устройствами PlugOS.Другими словами, даже если в клиентском приложении хост-машины обнаружится уязвимость, оно будет взломано хакерами или даже полностью взят под контроль, оно не сможет получить доступ к внутренним данным PlugOS или расшифровать их.

7.2. Обязанности и ограничения: что он может и чего не может делать

Для четкого определения границ его возможностей в таблице ниже подробно перечислены разрешенные функции клиентского приложения и действия, ограниченные архитектурой:

Разрешенные функции (что можно делать)	Ограничения архитектуры (что нельзя делать)
1. Передача ввода: прием сигналов ввода с клавиатуры, мыши, сенсорного экрана и т. д. хост-компьютера и их передача без изменений по каналу с сквозным шифрованием на аппаратное	1. Расшифровка любых данных: все ключи шифрования надежно хранятся в TEE/SE аппаратного обеспечения PlugOS и никогда не покидают аппаратное обеспечение. Приложение не может получить доступ к ключам, поэтому не

обеспечение PlugOS.	может расшифровать передаваемые им данные.
2. Отображение вывода: прием потока данных кадров изображения с экрана аппаратного обеспечения PlugOS и их отображение на экране хост-компьютера.	2. Доступ к данным в открытом виде: приложение выступает лишь в качестве канала связи PlugOS с внешним миром; оно не может определять конкретное содержание сетевой коммуникации.
3. Прокси-шифрование сети: в качестве сетевого выхода перенаправляет зашифрованный сетевой трафик от PlugOS в Интернет.	3. Выполнение основной логики: все основные вычислительные задачи, такие как аутентификация пользователя, шифрование и дешифрование данных, чтение и запись в файловую систему, запуск приложений и т. д., выполняются полностью внутри аппаратного обеспечения PlugOS. Приложение не участвует в каком-либо процессе принятия решений.
4. Проверка собственных обновлений: подключение к официальному серверу для проверки наличия новой версии приложения, не связанной с обменом пользовательскими данными.	4. Хранение пользовательских данных: приложение не хранит на хост-машине никаких внутренних пользовательских данных, настроек или состояния PlugOS. Оно разработано как бессостоятельное.

7.3. Граница безопасности: даже в случае взлома PlugOS не подвергается угрозе

Клиентское приложение находится за пределами доверенной границы PlugOS и относится к недоверенной зоне. Даже если приложение хост-машины будет злонамеренно изменено или полностью взломано хакером, оно не сможет расшифровать или похитить какие-либо внутренние данные PlugOS. Безопасность PlugOS обеспечивается за счет «независимого аппаратного обеспечения + системного шифрования + строгих границ», а не зависит от поведения клиентского приложения. Такая конструкция устраняет риски, связанные с доверием к закрытым приложениям хост-машины.

8. Управление безопасностью и персоналом

Безопасность PlugOS обеспечивается не только технической архитектурой, но и отлаженной системой управления и организации. Мы создали специальные команды по разработке, тестированию, обеспечению соответствия и реагированию на чрезвычайные ситуации, сформировав замкнутый цикл безопасности на всех этапах от разработки до эксплуатации.

- **Разработка и тестирование систем безопасности**: постоянное изучение передовых технологий в области безопасности в сочетании с многоуровневым тестированием и проверками на проникновение, что обеспечивает постоянное совершенствование защитных характеристик PlugOS.

- **Соответствие нормативным требованиям и управление**: следование глобальным нормам и отраслевым стандартам, строгий контроль за обработкой данных, соблюдение требований таких нормативных актов, как GDPR и PIPL.
- **Реагирование на чрезвычайные ситуации**: создание механизма быстрого реагирования, охватывающего предотвращение, устранение и отслеживание инцидентов безопасности, для обеспечения стабильности сервисов.
- **Управление персоналом**: на всех этапах — от найма и введения в должность до увольнения — сотрудники проходят строгую проверку анкетных данных, принимают обязательства по соблюдению конфиденциальности, получают допуск к информации соответствующего уровня и проходят обучение по вопросам безопасности, что гарантирует индивидуальную ответственность за информационную безопасность.

9. Управление циклом безопасной разработки

PlugOS внедряет требования безопасности и конфиденциальности во весь процесс разработки программного обеспечения, формируя систему управления SDL, соответствующую международным стандартам:

- **Требования и проектирование**: проводится моделирование угроз безопасности и оценка соответствия, показатели безопасности выносятся на ранние этапы, что позволяет избежать рисков на уровне архитектуры.
- **Безопасная разработка**: соблюдение международных стандартов безопасного программирования (NIST, ETSI, OWASP и др.) в сочетании с автоматизированными инструментами и ручной проверкой, что позволяет исключить распространенные уязвимости.
- **Тестирование безопасности**: проводится многоуровневое тестирование и проверка соответствия требованиям третьими сторонами, включая проверку уровня шифрования, механизмов защиты данных и тестирование на проникновение, с составлением профессионального отчета по безопасности.
- **Постоянная защита**: после выпуска продукта постоянно выпускаются обновления безопасности, отслеживаются уязвимости и быстро устраняются, что обеспечивает безопасность и контролируемость PlugOS на протяжении всего жизненного цикла.

10. Безопасная эксплуатация

Безопасность PlugOS проявляется не только на уровне технической архитектуры и механизмов, но и в непрерывной эксплуатации и поддержке, соблюдении нормативных требований и внешней сертификации, что соответствует самым высоким отраслевым стандартам безопасности. Мы глубоко понимаем, что основа доверия пользователей — это не просто самопровозглашение, а система управления безопасностью эксплуатации и поддержки, выдерживающая проверки, аудит и сертификацию.

10.1. Обновления безопасности и эксплуатация

PlugOS создал безопасный, прозрачный и отслеживаемый механизм обновлений:

- **Обновления с криптографической подписью:** все обновления имеют официальную

подпись и распространяются по зашифрованному каналу; перед установкой необходимо пройти проверку цифровой подписи и целостности, что предотвращает установку вредоносных обновлений.

- **Механизм дельта-обновлений:** при обеспечении безопасности уменьшается размер пакетов обновлений, что снижает влияние обновлений на пользовательский опыт.
- **Возможность быстрого отката:** при обнаружении проблем с совместимостью или потенциальных рисков пользователь может одним нажатием вернуться к предыдущей стабильной версии.
- **Выполнение с минимальными правами:** процесс обновления строго ограничивает права до минимума, чтобы сама служба обновлений не стала точкой входа для атак.

10.2. Центр реагирования на чрезвычайные ситуации в области безопасности

Мы убеждены, что открытое сотрудничество с сообществом специалистов по безопасности является ключом к повышению безопасности продукта. С этой целью мы создали стандартизированный центр реагирования на чрезвычайные ситуации в области безопасности продуктов, который обеспечивает пользователям поддержку на протяжении всего жизненного цикла продукта:

- **Техническая поддержка по вопросам безопасности:** мы предоставляем оперативный ответ и решения по проблемам безопасности, с которыми сталкиваются клиенты при использовании продукта, формируя замкнутый цикл взаимодействия между эксплуатацией и обслуживанием безопасности продукта и управлением безопасностью клиентов.
- **Программа вознаграждений за обнаружение уязвимостей**: мы активно поощряем и вознаграждаем исследователей в области безопасности, ученых и «белых хакеров» со всего мира за тестирование безопасности PlugOS. Мы учредили программу вознаграждений за обнаружение уязвимостей, в рамках которой предоставляем денежные вознаграждения отдельным лицам и командам, обнаружившим и ответственно сообщившим нам о действительных уязвимостях.
- **Открытая политика раскрытия уязвимостей**: мы разработали и обнародовали подробную политику раскрытия уязвимостей, предоставив сообществу исследователей в области безопасности четкий и безопасный канал для сообщения об уязвимостях. Мы обязуемся своевременно подтверждать и оценивать полученные сообщения, поддерживать связь с авторами сообщений и публично благодарить их после устранения уязвимостей.
- **Межотраслевое сотрудничество**: мы постоянно налаживаем каналы сотрудничества с поставщиками решений безопасности, научно-исследовательскими организациями и сообществами открытого исходного кода, чтобы своевременно получать информацию об угрозах и реагировать на них.

11. Контрольный список мер безопасности для пользователей

Чтобы помочь пользователям максимально использовать возможности PlugOS в области безопасности, мы рекомендуем регулярно проверять следующий контрольный список:

- **Хранение ключей продукта:** пользователи должны надежно хранить ключи продукта. Если вы опасаетесь утечки ключей продукта, вы можете сбросить их в настройках PlugOS.
- **Проверка привязанных хостов:** регулярно проверяйте в настройках список привязанных хостов и удаляйте устройства, которые больше не используются или не являются доверенными.
- **Минимизация прав доступа:** следуйте принципу «включать только по мере необходимости» и предоставляйте приложениям доступ к камере, микрофону, определению местоположения и другим конфиденциальным **функциям** только в случае необходимости**.**
- **Настройте белый список сетей:** для приложений, обрабатывающих особо конфиденциальные данные, используйте функции брандмауэра, чтобы ограничить их доступ к сети.
- **Включение защиты от взлома методом перебора:** в соответствии с оценкой рисков включите функцию автоматического самоуничтожения после N-кратного ввода неверного пароля и обязательно сделайте резервную копию данных.
- **Установите пароль на случай принуждения:** чтобы противостоять потенциальному риску физического принуждения, заранее установите пароль для режима маскировки.
- **Регулярно создавайте резервные копии данных:** данные бесценны, поэтому регулярно создавайте их резервные копии, чтобы предотвратить их потерю.
- **Обновляйте систему:** своевременно устанавливайте официальные обновления безопасности, чтобы обеспечить оптимальную защиту системы.

12. Заключение

PlugOS — это не просто продукт, а воплощение концепции безопасности. Опираясь на независимую и проверяемую аппаратную основу, а также сочетая многоуровневую архитектуру защиты и перспективный подход к защите конфиденциальности, PlugOS предоставляет пользователям настоящий цифровой сейф.

Благодаря своей проверяемой цепочке доверия на аппаратном уровне, независимой сертификации безопасности от третьих сторон, а также уникальной архитектуре «нулевого доверия» и механизму самоуничтожения данных, PlugOS предлагает надежное, мощное и прозрачное решение для пользователей, предъявляющих высочайшие требования к суверенитету данных и личной конфиденциальности. Мы уверены, что, полностью возвращая контроль пользователям, PlugOS устанавливает новые стандарты в области мобильной безопасности.