Безопасность «Интернета вещей», встроенная в карты памяти. Универсальное решение от Swissbit

По мере того как устройства, оборудование и промышленные предприятия становятся «интеллектуальнее», они также становятся более уязвимыми. При разработке и проектировании объектов, имеющих подключение к сети, разработчики должны уделять особое внимание аспектам информационной безопасности. Сегодня компания Swissbit предлагает очень гибкий аппаратный подход, который включает в себя TPM (Trusted Platform Module — доверенный платформенный модуль) и шифрование данных.

Универсальное решение Swissbit

Для обеспечения информационной безопасности и защиты данных компоненты системы, взаимодействующие через Интернет или через свои локальные IoT (Internet of Things — «Интернет вещей») шлюзы, должны обладать уникальным и некопируемым идентификатором. Системы также должны быть способны передавать, принимать и хранить криптографически защищенные данные. Решение, включающее в себя только применение программного обеспечения, редко обеспечивает достаточную защиту. Это ставит серьезные задачи перед разработчиками и производителями.

Компания Swissbit, являющаяся экспертом в области хранения и безопасности, предлагает новый аппаратный подход. Разработчики встраиваемых систем промышленного назначения знают компанию Swissbit как единственного независимого европейского производителя flash-памяти. Многие считают швейцарскую компанию, производящую продукцию в Германии, идеальным вариантом для приобретения надежных, долговечных твердотельных SSD-накопителей с PCI- и SATA-интерфейсами, CompactFlash, USB-устройств flash-памяти, карт памяти SD и microSD и управляемой памяти NAND BGA.

Полагаясь на многолетний опыт защиты хранимых данных, компания Swissbit разработала новый, более совершенный подход к защите встраиваемых IoT-устройств. Основная идея заключается в том, что каждому устройству необходима память для сохранения Log-файлов в журнал и сохранения данных из кэша в случае сетевых сбоев. Данные интерфейсы памяти могут и должны иметь средства защиты.

Защита в формате карт памяти

Новое решение по обеспечению защиты и безопасности компании Swissbit разработано на базе flash-памяти, производимой и тестируемой в соответствии с промышленными требованиями. Этот чип памяти работает с использованием специальной версии прошивки durabit со встроенным 256-битным AES-шифрованием. Продукты, входящие в состав серии DP (Data Protection — защита данных), обеспечивают шифрование и защиту всех данных различными способами (режим CD-ROM, защита с помощью PIN-кода, скрытая память, режим WORM). Аппаратная защита связи в IoT требует дополнительного модуля в карте памяти, который можно назвать еще одним якорем безопасности. Модули защиты компании Swissbit поставляются в комплекте с такими решениями, как интегрированные в накопители микросхемы Infineon/NXP CC EAL 5+/6+. Для разработки приложений в наличии имеются API, SDK и библиотека PKCS#11.

Определение идентификатора для вещей

Эксперты в области информационной безопасности заявляют,

что использование карт microSD со встроенным модулем шифрования обеспечивает надежную защиту данных, например передаваемых посредством мобильного телефона. Аналогично взаимодействию между людьми взаимодействие вещей в сети Интернет также требует применения идентификации, аутентификации и авторизации. Иными словами, как «вещь» узнает, что данные или запросы данных, получаемые от другой «вещи», корректны и что источник сообщения действительно является тем компонентом системы, за который он себя выдает? Продукция компании Swissbit с встроенным элементом безопасности обеспечивает приложения и системы своим уникальным идентификатором. «Вещи» получают защищенный от подделок идентификатор, и таким образом можно обеспечить защиту сетевых систем от неправомерного использования, «хищения идентификационных данных», а также можно ограничить доступ к данным. Модули, которые интегрируются в карты памяти, обеспечивают системы некопируемыми идентификаторами, преобразуя их в уникальных идентифицируемых участников взаимодействия M2M (машина-машина), которые могут аутентифицировать самих себя и передавать и получать криптографически и сильно защищенные данные.

Еще одним важным для устройств решением от компании Swissbit является приложение Trusted Boot. Trusted Boot гарантирует, что программное обеспечение сможет работать только на конкретном оборудовании или

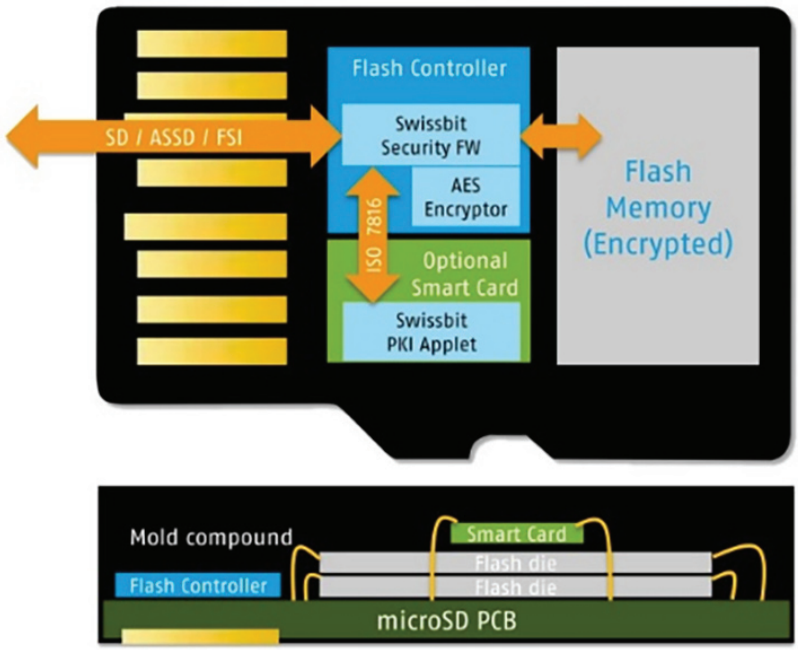


Рисунок 1. *Структура карты microSD с функциями безопасности*

группе устройств. Используя защищенные карты памяти с данной технологией, можно управлять лицензированием и активацией различных функций на устройствах. Управление доступом, шифрование кода или цифровая подпись обеспечивают возможность определения и управления различными конфигурациями ПО для продуктов.

Возможность модификаций и инноваций

В сравнении с припаянным TPM-модулем идея съемного модуля защиты на первый взгляд может показаться необычной. Тем не менее в более старом оборудовании и системах, как правило, имеется USB-интерфейс или интерфейсы для карт памяти. Поэтому большое преимущество применения съемных модулей защиты заключается в том, что существующие устройства можно легко модифицировать и обеспечить их защиту с помощью защищенной памяти компании Swissbit.

Такая возможность модификации устройств обеспечивает еще одно преимущество в постоянной гонке за кибербезопасностью. Методы

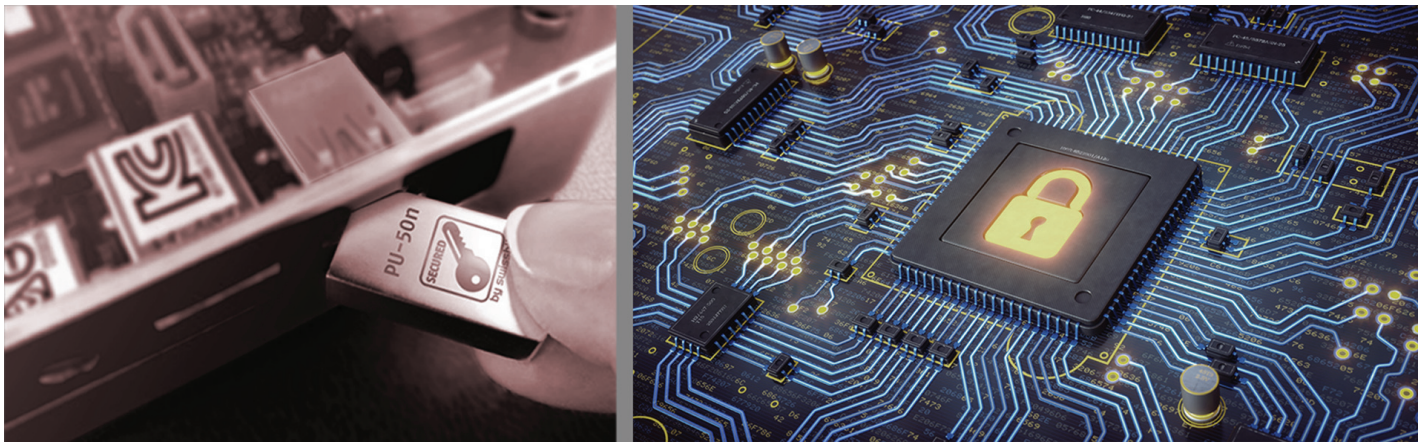


Рисунок 2. *Интерфейсы памяти, например USB, можно использовать для модификации функции доверенного платформенного модуля*

кибератак и защита от них развиваются циклически, и учесть их на протяжении всего жизненного цикла проекта промышленного предприятия является сложной задачей. Может возникнуть ситуация, когда необходимо присвоить новый идентификатор с улучшенными криптографическими технологиями участникам взаимодействия M2M. Модифицируемое решение компании Swissbit обеспечивает такую возможность.

Перспективы

В ответ на быстро растущую потребность рынка во встраиваемых IoT-решениях компания Swissbit открыла в октябре 2019 г. новое предприятие в Берлине. Этот завод оснащен самой современной передовой технологией 3D-упаковки микросхем, благодаря которой возможна разработка и производство индивидуальных конструкций «система в корпусе» и многочиповых модулей для клиентов компании. Данная технология упрощает интеграцию не только микроконтроллеров, чипов памяти NAND и криптографических модулей, но также датчиков, микросхем беспроводной связи и антенн. Использование карт памяти с TPM-модулем и блоком шифрования для обеспечения безопасности может быть только началом с возможностью добавления дополнительного функционала, которые можно миниатюризировать и интегрировать.

Актуальный пример технических средств защиты для систем кассовых терминалов

Структурное подразделение Swissbit по продуктам безопасности и IoT представило на одной из прошедших выставок свое решение TSE (Technical Security Equipment), позволяющее вести защищенную от несанкционированного доступа запись данных кассового аппарата.

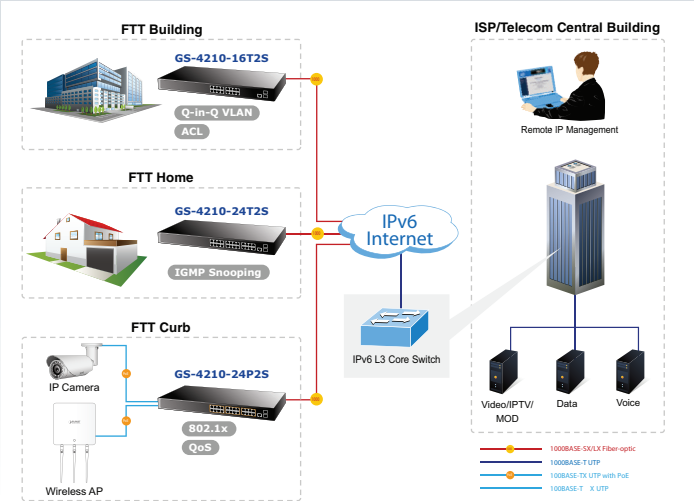
Управляемый промышленный коммутатор GS-4210-24T2S от Planet

Высокопроизводительный коммутатор GS-4210-24T2S с не блокируемой архитектурой выполнен в компактном металлическом корпусе. Новая модель представляет собой 24-портовый коммутатор, являющийся оптимальным решением для таких сфер применения, как видеонаблюдение (IP-камеры), беспроводные точки доступа и другие аналогичные устройства.

Коммутатор оборудован консолью, Web и SNMP-интерфейсами управления, что позволяет качественнее использовать сетевые ресурсы и гарантировать лучшую работу сети.

Технические характеристики

Модель	GS-4210-24T2S
Протоколы управления	Web browser/Telnet/SNMP v1, v2c, v3 HTTP/TFTP LLDP SNTP SSH, SSL
Количество портов: **10/100/1000BASE-T** **100/1000BASE-X SFP**	 24 2
Пропускная способность	38.6 Mpps @ 64 bytes
Входное напряжение	AC 100–240 В, 50/60 Гц
Выходная мощность	14 Вт
Размеры	445×207×45 мм
Температура эксплуатации	0…+50 C



https://planet.com.tw/en/product/gs-4210-24t2s