Обеспечение безопасности интеллектуальной собственности и защита конфиденциальной информации

Маркус ВОМФЕЛЬД (Markus VOMFELDE)
Брэд РЕКС (Brad REX)
Закари ЭЛЛИС (Zachary ELLIS)
Кимберли ДИНСМОР (Kimberly DINSMORE)

Обеспечение безопасности устройств с подключением к Интернету — задача комплексная и трудоемкая даже для опытных разработчиков. Если конечное устройство подсоединено к любой открытой сети, обменивается данными или обновляется через сеть, необходима защита от взлома и подмены данных. Позаботиться о построении надежной защиты крайне важно в самом начале, на этапе проектирования устройств. В статье приведены основные принципы обеспечения безопасности устройств, основанных на микроконтроллере. Компания Renesas Electronics, мировой лидер на рынке полупроводников, предлагает высокопроизводительные решения, базирующиеся на широком выборе микроконтроллеров, которые помогут при реализации проектов в области обеспечения безопасности, рассмотренных в данной статье.

«Безопасность» — слово, которое всегда вызывает интерес, но его значение может сильно меняться в зависимости от контекста, даже если рассматривать только электронные устройства (рис. 1). Для потребителя безопасность обычно означает, что персональные данные недоступны никому, кроме конкретных получателей, но для изделий с микроконтроллерным управлением зачастую имеется не так много данных конечного клиента, которым необходима защита. Рассмотрим некоторые другие определения слова «безопасность». Для разработчиков программного обеспечения безопасностью является отсутствие возможности кражи кем-либо их кода. Для производителей оригинального оборудования безопасность означает невозможность создания копии этого устройства. Для поставщиков услуг, предлагаемых через электронное устройство, безопасность синонимична невозможности использовать услуги без надлежащей авторизации или оплаты. Для правительств безопасность может заключаться в невозможности внедрения в устройство и использование его в качестве оружия в рамках DDoS-атаки.

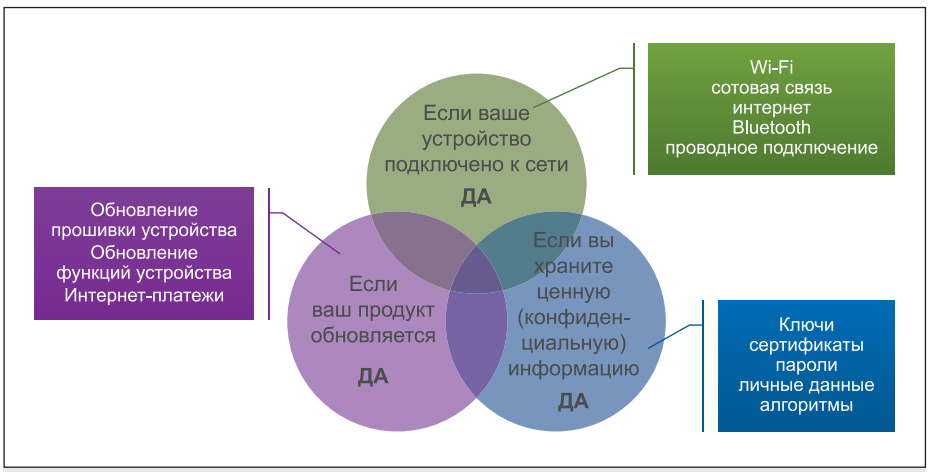

Рис. 1. Необходимо ли вам обеспечивать безопасность устройства?

Все эти определения, безусловно, относятся к микроконтроллерам и изделиям на их основе, независимо от сегмента рынка.

Для описания безопасности используется множество новых терминов и аббревиатур. Поэтапно рассмотрим данный вопрос, избегая при этом сложной лексики. Как обеспечить безопасность вашего устройства, основанного на микроконтроллере?

Этап 1: решения о безопасности принимаются перед началом проектирования

При разработке нового проекта высшее руководство компании хочет видеть прогресс, и для него это означает создание рабочего прототипа, однако прототипы могут не быть безопасными, и безопасность не бросается в глаза, чтобы произвести впечатление на руководство и инвесторов. Как бы ни было заманчиво отложить вопрос о безопасности до окончания проекта, нельзя поддаваться искушению. Да, это займет дополнительное время и для этого часто требуется переобучение руководства, но, как неоднократно было доказано, безопасность невозможно модифицировать в готовой конструкции. Безопасность не является дополнением; она имеет основополагающее значение для всей архитектуры устройства. Попытка

добавить ее позже почти всегда приводит к полной переработке конструкции: сформированный и побайтно переданный поток данных нельзя преобразовать в зашифрованный блок данных, жестко запрограммированные секретные ключи открытого текста не могут волшебным образом стать надежно хранимыми уникальными ключами устройства и так далее.

Этап 2: попадает ли ваш продукт под промышленное или государственное регулирование?

Это требование отменяет любые другие соображения о безопасности. Если для вашей отрасли необходим определенный набор криптографических функций, вы должны использовать именно его, даже при наличии альтернативных вариантов, которые обеспечивают тот же уровень защиты. Финансовые операции и счетчики энергии являются лишь двумя примерами, где существуют и должны соблюдаться эти правила. Убедитесь, что вы изучаете и принимаете любые нормативные требования для вашего изделия и уверены, что общегосударственные правила будут включены в те области, в которых предполагается использовать ваше изделие.

Этап 3: что вы хотите защитить?

Большинство компаний определяет этот список в соответствии со стоимостью, а потому издержки, касающиеся GDPR (General Data Protection Regulation, Генеральный регламент по защите персональных данных), весьма велики. Правительства понимают, что без финансовых стимулов велика вероятность стремления компаний устранять факты нарушения безопасности, чем пытаться предотвратить их. На первом этапе создания этого списка обычно сосредоточиваются на самом устройстве и данных: прошивках, ключах и клиентской информации, но желательно заглянуть за пределы устройства и рассмотреть систему в целом. Вы можете не считать ваши данные конфиденциальными, но не удастся ли кому-то еще использовать ваше устройство и не приведет ли это к столь пагубным последствиям, как DDoS-атака? Если устройство отвечает за критически важную функцию, необходимо защитить ее от всего, что может неправильно изменить ее. Если ключи применяются для запуска некой службы, то служба сама по себе подлежит защите.

Этап 4: каковы ваши уязвимости?

Вновь рассмотрим устройство и его развернутую инфраструктуру. При этом очевидно, что подключение к Интернету технически уязвимо. Это часто снижает стоимость изделий на основе микропроцессора, поскольку, как правило, мишенью взломщиков являются не Linux IP-соединения, и значение передаваемых данных можно оспаривать, но если вы обновляете прошивки через Интернет и хотите защитить свой код, то IP-соединение становится уязвимым. Даже если устройство не имеет IP-соединения, надо рассмотреть все остальные соединения с внешним миром. При анализе рабочей среды изделия следует также учитывать человеческий фактор. Печальная реальность состоит в том, что современную технологию обеспечения безопасности иногда можно полностью обойти, использовав хорошо спланированный подкуп, и надо помнить, что злонамеренный или просто озорной человек способен сделать это.

Этап 5: кому вы доверяете?

Хорошо известно выражение «не доверяй никому», но нельзя не принять во внимание тот факт, что решения безопасности увеличивают себестоимость, а потому не тратьте деньги на защиту вашего продукта от несуществующей угрозы. Если ваше производство расположено в месте эксплуатации, по-видимому, нет необходимости в инвестировании в безопасное программное решение. Однако если программирование устройства осуществляется за пределами места эксплуатации или вам нужно запрограммировать устройство с ключами или другими конфиденциальными данными, может потребоваться безопасное программное решение.

Этап 6: определите свои ограничения

Все можно нарушить/взломать при наличии достаточного времени и ресурсов. Вы должны решить, какой объем защиты вам требуется. Защита от нежелательного доступа через интерфейс отладчика — это одно; защита от снятия кем-либо микроконтроллера с платы и анализа чипа электронным микроскопом — совсем другое. Иногда эти ограничения регламентируются органом, контролирующим производство вашего изделия, но, как правило, они определяются просто здравым смыслом. Например, если ваша основная цель в том, чтобы защитить лишь интеллектуальную собственность вашей встроенной программы, то нет необходимости использовать микроконтроллер, защищенный от доступа по другим каналам.

Этап 7: составьте план

Решите, как вы будете защищать свои ресурсы от уязвимостей, используя элементы, которым вы доверяете, в пределах установленных ограничений. Иногда усилия, относящиеся к модели угроз, их анализу, оценке безопасности или политике безопасности, представляют собой время, затрачиваемое на то, чтобы должным образом сосредоточить внимание на достижении цели и бюджете. Этот последний этап также важен в случае, если что-то пойдет не так. Если вы доказали, что надлежащим образом оценили все потребности в безопасности продукта, это может помочь оспорить предъявленные вам претензии в проявлении халатности.

Сочетание угроз, уязвимостей и доверенных участников столь же разнообразно, как и количество встроенных устройств, но, к счастью, есть некоторые общие темы и частично совпадающие решения.

Защита данных в местах хранения

Основополагающим требованием безопасности является возможность безопасного хранения данных на устройстве, но, как и все в этой сфере, безопасное хранение имеет различные аспекты. Если у вашего устройства отсутствует внешнее подключение, микропроцессорный блок защитить довольно просто, отключив или защитив доступ ко всем входам отладчика и программатора. Если вам нужно убедиться, что устройство не может непреднамеренно повредить себя, перепрограммировав свою флэш-память, то многие микроконтроллеры имеют возможность назначить одноразовый пароль на часть или на всю флэш-память, предотвращая ее от стирания и/или перепрограммирования даже с помощью самопрограммирования. Однако если устройство имеет внешнее подключение, можно логически разделить свой код и данные на категории доверенных и ненадежных, а также обеспечить доступ к доверенным данным только с помощью специального кода. Оптимально это разделение должно быть аппаратно-принудительным с помощью механизма, такого как блок защиты памяти (Memory Protection Unit, MPU) или Arm Trust'one. Хотя подобное разделение не обеспечивает полной безопасности, оно позволяет уменьшить атакуемую зону для доверенной области.

Идентификация устройства

Если изделие будет подключено к инфраструктуре, вам понадобится какой-либо способ его однозначной идентификации. Существует множество методов, чтобы придать каждому устройству уникальную идентичность. Некоторые микроконтроллеры уже имеют встроенные уникальные идентификаторы, но в них, как правило, прослеживается тенденция к простой сериализации, которая затем должна быть отображена так, чтобы центральный командный центр мог распознать, где какое устройство используется. Хотя это может быть удобно, но предпо-

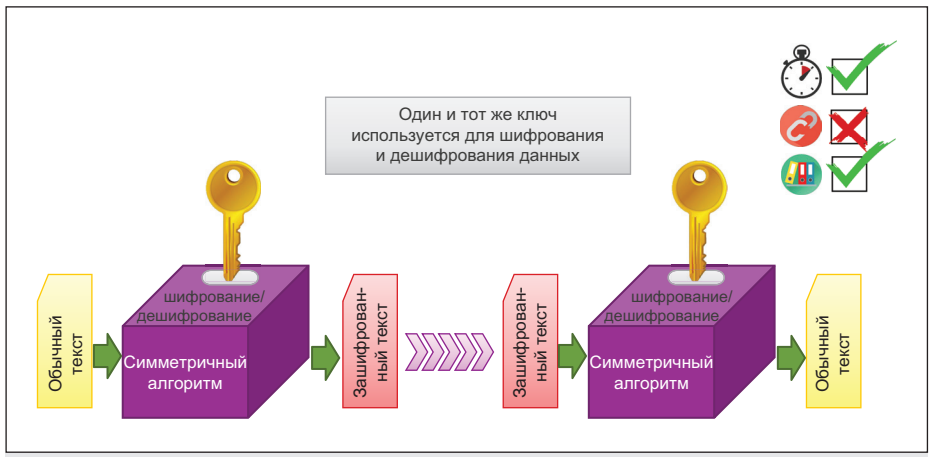

Рис. 2. Симметричное шифрование

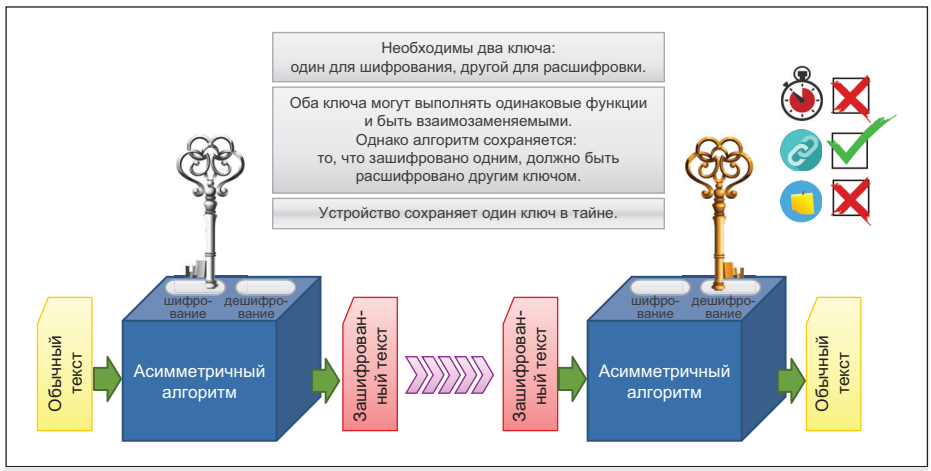

Рис. 3. Асимметричное шифрование

чтительнее уникальная криптографическая идентификация, поскольку она позволяет принимать дополнительные решения в области безопасности, такие как защита данных в процессе обмена.

Криптографическая идентификация использует методы различных схем шифрования, при этом идентичность устройства подтверждается ключом шифрования. Есть два основных варианта:

- Симметричное шифрование (шифрование с одним ключом), где один и тот же ключ предусмотрен и для шифрования, и для расшифровки данных. Командный центр должен знать симметричный ключ для каждого устройства (рис. 2).
- Асимметричное шифрование (шифрование с открытым ключом), где один ключ используется для шифрования данных, а другой — для расшифровки. Функции взаимозаменяемы, что позволяет устройству сохранять один ключ в тайне (рис. 3).

Небольшая сложность состоит в том, как изначально получить ключи на устройстве так, либо чтобы ключ был известен командному центру, либо чтобы ключ являлся доверенным. Это называется инициализацией. Если в соответствии с оценкой безопасности вы делаете вывод, что изделие может устанавливать и инициализировать доверенный специалист, то можете вводить ключи или даже генерировать их на месте. Однако если изделие предназначено для установки обычным потребителем, то необходимо обеспечить безопасность устройств. Это можно сделать во время безопасного программирования.

Защита данных в процессе обмена

Существует пять целей для обеспечения безопасности данных в процессе обмена: конфиденциальность, целостность данных, источник данных, аутентификация объекта и невозможность отказа. Обсуждение этих вопросов выходит за рамки нашего обзора. Основное внимание здесь следует уделить тому, чтобы определить, что такое коммуникационная инфраструктура. Если устройство соединяется через собственную шину в замкнутой инфраструктуре, у вас будет гораздо больше разных решений, позволяющих удовлетворить эти требования, чем если ваше устройство подключено к Интернету через Wi-Fi-соединение. Последний случай является наихудшим сценарием, но это также и наиболее распространенный вариант для IoT-устройств. Фундаментальным элементом защиты данных в процессе обмена через IP-соединение является криптографическая идентичность. Хотя криптографическая идентичность может показаться несколько излишней, это становится необходимым требованием, если ваше изделие подключено через IP-соединение.

Безопасное программирование

Как и большинство решений в области безопасности, безопасное программирование способно решить множество проблем, и существует большое количество доступных вариантов. Размещение производства в безопасном месте может предотвратить кражу интеллектуальной собственности (IP), клонирование и незаконное производство, позволяя вам получить образ прошивки в зашифрованном формате, который может расшифровать только конкретный программист этого устройства, а также получить аудиторский отчет о точном количестве запрограммированных устройств. Существуют также безопасные программные решения, при которых в микропроцессорный блок могут быть введены уникальные ключи устройства. Известны даже передовые решения, где микропроцессорный блок сам генерирует асимметричную пару ключей, экспортирует открытый ключ, а также получает и хранит подписанный сертификат, содержащий этот открытый ключ, формирует как аудиторский отчет, так и группу утвержденных сертификатов, которые могут быть использованы для проверки подлинности конечного изделия. Этот аспект, в частности, требует существенной технической поддержки микропроцессорного блока со стороны партнеров по экосистемам.

Обеспечение безопасности интеллектуальной собственности и защита конфиденциальной информации

Итак, мы привели общий обзор мер по обеспечению безопасности устройств для глобально связанного мира. Теперь рассмотрим более подробно требования и методы защиты данных в микропроцессорном устройстве или в приложении. В приведенном примере, описывающем вымышленную ситуацию, будут рассмотрены различные уровни безопасности, основанные на требованиях приложения и сценариев потенциальных атак. Это должно помочь подготовить план обеспечения безопасности хранящихся в устройстве данных и на основании ваших требований найти наилучший уровень безопасности.

Зачем защищать локальные данные?

Существует два различных типа сохраняемых в устройстве данных — прикладная про-

грамма, которая будет выполняться во время работы, и локальные данные, применяемые во время работы. Прикладная программа содержит интеллектуальную собственность, и поэтому изготовитель устройства защищает свою информацию от кражи, повторного использования или копирования.

Локальные данные обычно хранятся в устройстве. Они могут передаваться на отдельное аналогичное устройство и обновляться, поскольку атрибуты всех устройств одинаковы. Локальные данные формируются во время установки устройства в оборудование или во время его эксплуатации. Содержащиеся во всех устройствах данные отличаются друг от друга и, как правило, обновляются чаще, чем прикладная программа. Большая часть данных защищена от пользователя устройства, так как они могут содержать конфиденциальную информацию для оборудования в целом. Несмотря на то что защита данных может иметь разную мотивацию, требование к защите доступных сведений обязательно для обоих типов.

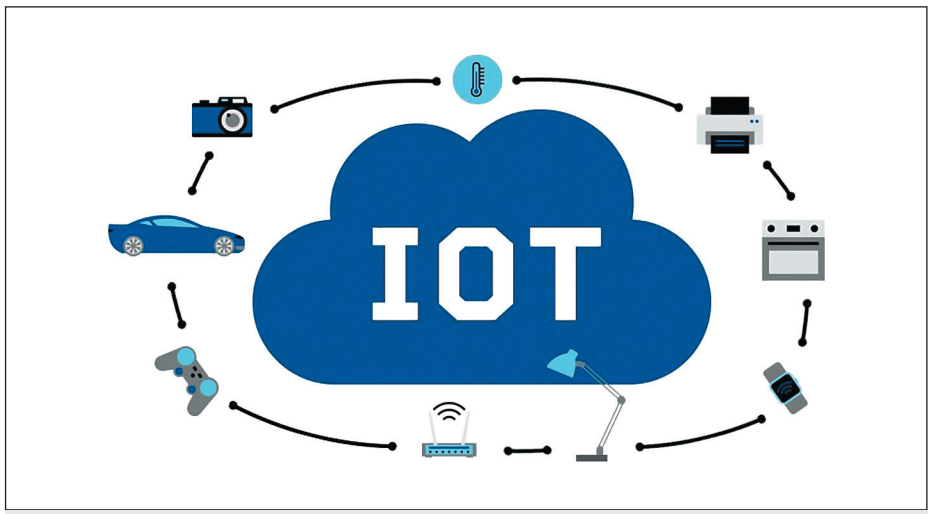

Рис. 4. Защита IoT-устройств

Подключено ли устройство к сети?

Это очень важный вопрос для обеспечения безопасности. Для автономного решения, которое работает без подключения к другим устройствам, возможны только атаки, связанные с непосредственным физическим доступом. Защита интеллектуальной собственности устройства по-прежнему остается проблемой для производителя, но несанкционированный доступ к пользовательским данным гораздо менее вероятен, ведь устройство обычно физически недоступно для взломщика. Устройство, работающее в местной замкнутой сети без выхода в Интернет, относится к следующему уровню подключения. Здесь взломщик должен получить доступ к сети до начала атаки на устройство, но и оно само также должно быть защищено от внешнего доступа и не стать точкой входа в замкнутую сеть. И наконец, максимальный уровень защиты нужен для устройства с непосредственным подключением к Интернету, так как число потенциальных взломщиков уже не ограничивается локальной сетью и взлом может быть осуществлен глобально и с почти бесконечной вычислительной мощностью. Кроме того, подобные атаки будут возрастать, чтобы получить доступ к хранящимся в устройстве данным (рис. 4).

Пример применения и требований к безопасности

Для того чтобы конкретизировать задачу, рассмотрим пример возможного применения, отражающего требования безопасности, предъявляемые к реальным ситуациям. Скажем, у нас есть дверной замок с датчиком отпечатков пальцев, чтобы ограничить доступ к зонам здания компании, куда посторонним вход воспрещен. Расположенный внутри устройства датчик с весьма малым объемом памяти имеет очень «умный» алгоритм хранения отпечатков пальцев 50 пользователей, наиболее часто посещающих это зону. Такое свойство делает его наиболее привлекательным для клиентов на рынке. Для других пользователей устройство подключается через Wi-Fi-сеть компании к серверу и проводит сравнение с хранящимися там отпечатками пальцев, а так как для предоставления права доступа требуется больше времени, то хранящиеся внутри устройства данные имеют реальное преимущество. Сеть Wi-Fi тоже имеет доступ к Интернету, чтобы быть готовой к получаемым от производителя обновлениям устройства по беспроводному протоколу. Как производитель устройств, вы должны подготовить план обеспечения безопасности для вашего случая. Здесь мы сосредоточимся на хранящихся в устройстве данных и не будем учитывать данные, которые будут меняться при операциях обновления информации или при дистанционном перепрограммировании. Первый тип защищаемых данных — это IP (интеллектуальная собственность) алгоритма отпечатков пальцев. Он является свойством самого устройства и должен быть защищен от любого проникновения, который может получить взломщик (при непосредственном или удаленном доступе). Поскольку устройство подключено к сети, недостаточно только защитить микроконтроллер от считывания, копирования или перепрограммирования. Кроме этого, необходимо защитить межсетевой протокол, чтобы взломщик, подключившись к сети, не смог извлечь данные из памяти. Второй тип данных в нашем примере, который следует учитывать,— это данные пользователей, сохраненные отпечатки пальцев и данные доступа к сети. Как сказано выше, физический доступ взломщика к устройству достаточно труден. Проникновение через Интернет более вероятен, поэтому нуждается в лучшей защите от атак. Частично это обеспечивается пользователем и защитой сети; однако для полной безопасности должна быть обеспечена защита внутри устройства.

Защитите свою интеллектуальную собственность (ИС)

Приведенный пример показывает, что существует несколько составляющих безопасности, необходимых для защиты хранимых данных. Чтобы сосредоточиться на безопасности данных, мы предполагаем, что используется устройство с защищенной подлинностью, которому можно доверять. В следующей статье из этой серии будет разъяснено, какой тип микроконтроллера потребуется. Что касается защиты интеллектуальной собственности, должно обеспечиваться несколько уровней защиты, которые зависят от выбранного плана безопасности и требуемого объема защиты. На первом этапе обеспечения безопасности выбранный микроконтроллер должен поддерживать защиту от нежелательного доступа со стороны отладчика и программатора. Есть множество способов для достижения этой важной защиты, и необходимо выбрать один из них на основании их сравнения. Разные поставщики используют разные методы защиты, имеющие различные возможности для обеспечения безопасности. Необходимо убедиться, что эта реализация рекомендуется для обеспечения безопасности, а не только для предотвращения непреднамеренной модификации устройства. Следующий этап — это использование микроконтроллера, позволяющего поддерживать различные зоны доступа, которые являются либо доверенными, либо нет. Это позволит избежать прямого доступа микропроцессорного ядра к хранилищу ИС, а потому извлечь данные из памяти просто невозможно. Наиболее распространенное решение — реализация блока защиты памяти, который мог бы быть применен для описанных выше целей или реализации Trust'one для ARM-микроконтроллера. Наконец, можно хранить ИС-данные в зашифрованном виде

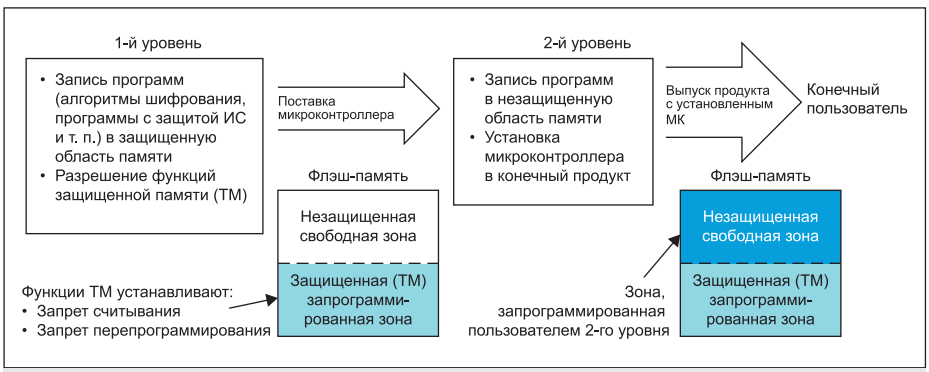

Рис. 5. Пример многоуровневой зоны доверенной памяти

на устройстве. Это сделает его гораздо более устойчивым к физическим атакам, поскольку отсутствует энергонезависимая память, в которой в качестве читаемых данных хранится интеллектуальная собственность, и ее невозможно считать с помощью инкапсуляции или анализа электронным микроскопом. Таким же образом хранящийся в микропроцессорном блоке ключ шифрования должен быть защищен от считывания прямым доступом из процессора и надежно храниться, чтобы не допустить считывания ключа и зашифрованного ИС-контента с целью получения доступа к секретной информации. Если вы храните зашифрованный алгоритм, его следует расшифровать в оперативной памяти устройства и выполнить оттуда. Это наиболее безопасный способ хранения интеллектуальной собственности, но также необходимо включить ту часть оперативной памяти, в которой хранится алгоритм, в доверенную область памяти микропроцессора.

Защита данных, сохраняемых в устройстве

На втором этапе необходимо определиться с данными, которые конечный потребитель будет хранить в устройстве. В нашем примере информация об отпечатках пальцев была сохранена, чтобы получить быстрый доступ к защищенной зоне, а также к клиентской сети, чтобы обеспечить подключение к серверу, где находятся все данные об отпечатках пальцев. Это также позволит в дальнейшем производителю обновлять прошивки. В принципе можно использовать те же самые меры безопасности, как и для хранящегося в устройстве интеллектуального продукта. Мы хотим подробнее изучить этот вопрос и принять решение об обязательном уровне безопасности в эксплуатации. Устройство должно быть защищено даже от частичного считывания или перепрограммирования, чтобы избежать установки любых вредоносных программ, способных предоставить взломщику сетевой доступ к данным. Кроме того, разделение памяти на доверенные и ненадежные области имеет очень большое значение, поскольку ограничит возможность микропроцессорному блоку получать доступ к хранимым данным.

Это усложнит любую атаку и создаст повышенную защиту при незначительном снижении работоспособности. В конечном счете шифрование данных является обязательной мерой, хотя и будет отрицательно влиять на работоспособность. Все сохраненные отпечатки пальцев должны быть расшифрованы до начала работы алгоритма, а значит, этот вклад в работоспособность должен учитываться заранее. С другой стороны, физический доступ к устройству внутри помещения заказчика может быть весьма затруднен, что следует учитывать, если подобное требование становится обязательным. Что может сделать взломщик с хранимыми данными отпечатков пальцев до тех пор, пока алгоритм сравнения недоступен? Но для доступных по сети данных это не так. Здесь отрицательное влияние на работоспособность практически отсутствует, так как операция производится один или два раза в день, но если кто-то сможет взять устройство и считать код доступа к сети как незашифрованные данные, то получит полный доступ к клиентской сети. Это может стать более опасным, причем с непредсказуемым результатом. Опять же необходимо подчеркнуть, что хранение ключа шифрования должно обеспечиваться с большей безопасностью, чем хранение самих данных во избежание любого нежелательного доступа к зашифрованной информации. Очень эффективный способ сделать это — применение уникального ключа для каждого микропроцессорного блока. Но указанная тема не входит в обсуждение данной статьи.

Решение о том, как и на каком уровне следует обеспечивать безопасность, всегда зависит от условий использования, ожидаемых взломщиков и их доступа к устройству или данным, которые должны быть защищены. Другими словами, для каждой реализации безопасности команда разработчиков должна рассматривать этот вопрос в самом начале проекта, чтобы принять важное решение для микропроцессорного блока, подходящее для всех требований обеспечения безопасности. Приведенный здесь пример показывает широкий выбор функций безопасности для данных локального хранения, и этот набор будет увеличиваться с дополнительными функциями для передаваемых данных или для безопасного беспроводного программирования.

Многоуровневая зона доверенной памяти

Пример формирования многоуровневой зоны доверенной памяти (TM, Trusted Memory) для МК семейства RX приведен в [1], где подробно рассмотрено создание такой зоны во флэш-памяти в среде разработки E2Studio (рис. 5).

Имеется три уровня доступа/защиты:

- Изготовитель микроконтроллера или партнер пользователя второго уровня, зашивающий в МК собственные алгоритмы (например, криптозащиты), с защитой интеллектуальной собственности на них.
- Пользователь микроконтроллера — изготовитель конечного оборудования. Не имеет доступа к копированию/изменению программ первого уровня, но имеет возможность зашить в контроллер собственную программу и защитить ее от взлома/копирования.
- Пользователь конечного оборудования.

Продукты компании Renesas

Семейство 32-разрядных микроконтроллеров Renesas RA с ядром ARM Cortex-M

Это лидирующие в отрасли 32-разрядные микроконтроллеры с процессорными ядрами ARM Cortex-M33, -M23 и -M4, сертифицированные как PSA (Platform Security Architecture). МК RA обладают многими ключевыми преимуществами по сравнению с микроконтроллерами ARM Cortex-M других производителей.

Средства обеспечения безопасности семейства RA6, интегрированные в микроконтроллер:

- шифрование AES128/192/256 с возможностью генерации симметричных и несимметричных ключей и их сохранения;
- функция хеширования GHASH;
- поддержка алгоритмов:
  – 3DES/ARC4,
  – SHA1/SHA224/SHA256/MD5,
  – RSA/DSA/ECC;
- генератор истинно случайных чисел (TRNG);
- уникальный идентификатор;
- механизмы защиты памяти.

Семейство 32-разрядных микроконтроллеров RX с высокой энергоэффективностью

Семейство состоит из четырех серий: флагманской серии RX700 с самой высокой производительностью и наиболее продвинутыми функциями; стандартной серии RX600; серии RX200, которая обеспечивает оптимальный

баланс энергоэффективности и высокой производительности; серии RX100 начального уровня с чрезвычайно низким энергопотреблением. Линейка микроконтроллеров обеспечивает масштабируемость от небольших до весьма крупных приложений.

Программно-аппаратная платформа Synergy

Содержит четыре отдельные серии микроконтроллеров и полный набор коммерческого ПО (RTOS, драйверы и коммуникационные стеки). Платформа предназначена для конечных приложений — от подключенных мобильных устройств для рынка IoT до высокопроизводительных контроллеров встраиваемых систем. Благодаря широкому спектру производительности, функций, а также совместимости по выводам в каждой серии микроконтроллеры Synergy обеспечивают потребности в масштабируемости, низком энергопотреблении, повторном использовании кода и необходимой производительности для рынка встраиваемых систем.

Заключение

Безопасность — это не утверждение того, что для всех подходит один формат. Очень важно определить конкретные требования к изделию перед началом разработки и выбрать микроконтроллер с необходимыми аппаратными возможностями, программной поддержкой и демонстрацией решений, поддерживаемых поставщиком микросхем с сильной партнерской сетью. Безопасность может показаться пугающе сложной, но выбор правильного микроконтроллера, поддерживаемого надежной экосистемой, позволит создать безопасный продукт для сегодняшнего глобально связанного мира.

Обеспечение безопасности устройств с подключением к Интернету — комплексная задача. Если конечное устройство подключено к любой открытой сети, обменивается данными или обновляется через сеть, необходима защита от взлома, перехвата и подмены данных. На уровне проектирования устройств важно в самом начале заложить «кирпичики» защиты. Компания Renesas предлагает мощный инструментарий — изолированные блоки памяти Flash и ОЗУ, аппаратное шифрование в независимых блоках Trusted Secure IP и Secure Crypto Engine, защищенный уникальный номер чипа и генератор случайных чисел. Кроме этого, Renesas использует схему ARM TrustZone в своих микроконтроллерах на ядрах ARM Cortex-M и Cortex-A. Компания получила сертификат ARM “PSA Certified level one” и участвует в сообществах Trusted Firmware M и Trusted Firmware A для развития программно-аппаратных средств защиты устройств IoT.

Компания Renesas Electronics, мировой лидер на рынке полупроводников, предлагает наилучшие и высокопроизводительные решения, основанные на широком выборе микроконтроллеров, которые помогут при реализации проектов в области обеспечения безопасности, рассмотренных в данной статье. Более подробную информацию о продуктах и решениях можно узнать на сайте производителя [2].

Литература

1. Использование функций доверенной памяти. **www.renesas.com/eu/en/doc/products/mpumcu/apn/rx/013/r01an2618ej0300_flash.pdf**
2. **www.renesas.com**