Безопасность в сетях IoT: Wi-Fi – это дёшево или сердито?

Илья Чепурин (Москва)

В статье рассматриваются основные аспекты безопасности, связанные с реализацией Wi-Fi-соединений для встраиваемых систем. Также уделяется внимание не только потенциальным уязвимостям, но и аппаратным возможностям элементной базы для построения защищённых систем, а также основным принципам их разработки.

24 июля 2016 г. на новостных лентах многих информационных агентств появилась новость о том, что Chrysler отзывает 1,4 млн автомобилей после сообщений о взломе информационной системы модели Jeep Cherokee [1]. Два специалиста по компьютерной безопасности, Чарли Миллер и Крис Валасек, опубликовали результаты своего исследования, в ходе которого они смогли через информационную систему Uconnect® получить полный доступ к управлению автомобилем [2]. Из отчёта следовало, что они смогли взломать пароль Wi-Fi для подключения к головному устройству мультимедийной системы. После этого, зная, какие параметры использует система для связи с провайдером, они смогли получить доступ к машине уже при помощи мобильной связи. И это было ещё не всё. Несмотря на заверения производителя о том, что мультимедийная система и внутренняя CAN-сеть автомобиля изолированы, они нашли уязвимое место – «парня, который знает другого парня» – контроллер, подключённый к CAN-шине, и способный, в то же время, общаться с головным устройством. Оказалось, что этот контроллер можно перепрограммировать, в результате чего появилась возможность с его помощью посылать команды по CAN-шине и, находясь в зоне покрытия сотовой связи, не только управлять автомобилем, но и отслеживать его координаты, что Чарли с Крисом и продемонстрировали журналистам издания Wired.

Как было упомянуто, всё началось со слабого пароля Wi-Fi. В теории идея была хороша: пароль генерировался автоматически, исходя из времени, когда автомобиль и его мультимедиа-система включались в первый раз. Комбинация из даты и времени суток с точностью до секунды – вполне надёжный пароль, для взлома которого потребовался бы перебор огромного количества вариантов. Однако, зная год и месяц производства машины, это число уменьшается до примерно 15 млн, а если предположить, что выпуск осуществляется только в рабочее время, то выбор сократится уже до 7 млн возможных кодов. На деле всё оказалось ещё проще: перед первым запуском системы она использует настройки по умолчанию – ровно полночь 1 января 2013 г. Поэтому пароль был прост – упомянутое время, плюс время загрузки головного устройства. Итогом такой непродуманности стал отзыв почти 1,5 млн автомобилей и огромный ущерб репутации компании.

Другой нашумевший случай произошёл совсем недавно, в октябре 2016 г., и уже стал известен как одна из самых массированных DDoS-атак [3]. В результате серверы Twitter, Amazon, Tumlbr, Netflix, Reddit и Spotify, подключённые к инфраструктуре провайдера Dyn, стали недоступными для пользователей. «Виновниками» оказались множество видеорекордеров и IP-камер, подключённых к интернету [4]. Специальный скрипт находил эти устройства в сети и, используя базу паролей по умолчанию, получал к ним доступ с возможностью управления. Специалисты называют эту атаку первым случаем, когда в качестве атакующего выступали не заражённые компьютеры, а встраиваемые системы с подключением к глобальной сети, т.е. то, что мы теперь называем Интернетом вещей (Internet of Things, IoT). Учитывая тот факт, что на данный момент количество проданного оборудования измеряется миллионами, можно себе представить масштабы угроз со стороны вроде бы безобидной электроники, которая, вследствие уязвимости к атакам злоумышленников, способна создать большие проблемы.

Такое происходит довольно часто, когда новые технологии развиваются семимильными шагами и средства информационной безопасности не поспевают за их развитием, или им просто не уделяется должное внимание. Технологии облачных сервисов будут развиваться и далее. Они уже прочно вошли в обиход, и количество устройств с подключением к Интернету будет только увеличиваться. По прогнозам разных аналитиков уже к 2020 г. в мире IoT будет насчитываться около 30 млрд электронных приборов.

Многие разработчики встраиваемых систем не являются экспертами в области информационных технологий, поэтому им зачастую сложно даже представить себе возможные риски и их последствия.

Для беспроводных устройств можно выделить три аспекта обеспечения безопасности:

- безопасность подключения к сети – как устройство идентифицирует сеть для подключения, как происходит аутентификация устройства в сети и как защищается канал связи с точкой доступа;
- безопасность коммуникационного канала – каким образом устройство подключается к различным сервисам (веб-серверам или другим системам) и каким образом происходит обмен данными;
- безопасность функционирования – как устройство ведёт себя при отсутствии связи с точкой доступа и то, каким образом происходит его настройка и обслуживание (изменение параметров конфигурации, обновление ПО и т.п.).

Кроме того, важно понимать, что рано или поздно любая система защиты будет обойдена (взломана), и весь вопрос состоит только в том, насколько серьёзными будут последствия. Мы все знаем закон Мёрфи, который гласит: «Если неприятность может случиться, то она обязательно случится». Применительно к описанным ситуациям он может звучать и так: «Если есть возмож-

ность использовать более слабую систему защиты или более слабый пароль, то они будут использованы».

Безопасность Wi-Fi

Процесс подключения к точке доступа состоит из двух этапов:

- аутентификация – то, как устройство и точка доступа представляются друг другу;
- шифрование – то, каким образом кодируются данные, передаваемые между устройством и точкой доступа.

На первом этапе устройства прослушивают эфир в поиске широковещательных пакетов с идентификатором сети SSID, рассылаемыми точками доступа, и, выбрав нужную сеть, подключаются при помощи пароля (ключа) или по протоколу EAP, когда подлинность устройства проверяется внешним сервером. Идентификатор SSID можно скрыть, что является одной из защитных мер, но как только в сети появляется клиент, который подключается к такой точке доступа, становится возможным узнать SSID.

Для защиты беспроводного подключения используется ряд протоколов, наиболее современные из которых – это WPA и WPA2. В устаревшем протоколе WEP использовался 40-битный ключ для шифрования, и на данный момент уже многократно продемонстрировано, что даже при использовании протокола TKIP и увеличении длины ключа, он всё равно достаточно легко взламывается. В основе наиболее современного протокола WPA2 лежит алгоритм шифрования AES с длиной ключа 128 или 256 бит. Однако немногие знают, каким образом этот ключ получается и используется. WPA2 предусматривает два режима работы:

- Personal с предварительно определённым ключом (Pre-Shared Key, PSK);
- Enterprise, в котором ключ является динамическим и уникальным для каждого подключения (за его генерацию отвечает сервер авторизации, чаще всего это RADIUS-сервер).

В первом случае мы имеем дело с наиболее широко распространённым вариантом подключения, который обычно используется в домашних сетях и в общественных местах. Мы привыкли к тому, что на смартфоне просто набираем пароль доступа и всё, мы подключены. Очевидное преимущество данного варианта – его простота, поэтому такой режим подключения реализован в подавляющем большинстве встраиваемых Wi-Fi-модулей или в микросхемах многих азиатских производителей. Они дёшевы в силу их массового применения, в том числе и в мобильной технике (смартфонах, планшетах и прочих гаджетах), поэтому и пользуются большой популярностью у многих разработчиков систем IoT или устройств для Умного дома. Однако не всё так просто. При использовании ключа PSK все устройства в сети имеют один и тот же пароль, который зачастую просто программируется, иногда даже без возможности его смены. Если по какой-то причине пароль сети стал известен постороннему пользователю или устройство было украдено, то для защиты системы необходимо срочно менять ключ на всех устройствах. Если для умного дома их количество пока может быть не более десяти, то в промышленных или офисных системах их число может достигать нескольких сотен и даже тысяч, при этом не все датчики могут находиться в легкодоступных местах. Представьте себе радость IT-персонала, вынужденного каким-то образом решать проблему изменения ключа – ведь помимо самой смены ключа нужно, чтобы вся система продолжала функционировать. А как это сделать, если в точках доступа пароль уже изменён, а оконечные датчики или исполнительные устройства ещё не перепрограммированы?

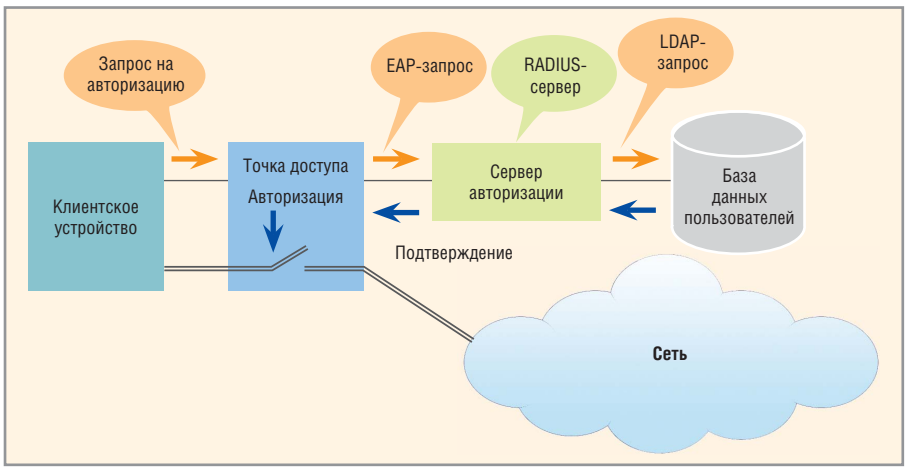

Рис. 1. Схема подключения по протоколам EAP в режиме Enterprise

Другим источником опасности являются различные Wi-Fi-снифферы и программные утилиты для подбора паролей к сетям Wi-Fi. Уже упоминалось, что для подключения к Wi-Fi-сети иногда достаточно просто знать пароль, установленный по умолчанию. Удивительно, но факт – многие пользователи, привыкнув к технологии Plug-and-Play, даже не задумываются о смене пароля на домашней точке доступа после её приобретения. А высока ли квалификация обслуживающего персонала в небольших офисах или торговых комплексах, где владелец вдруг решил внедрить управление через Интернет? Всё осложняется тем, что несанкционированное подключение к сети очень трудно отследить. При этом в сети с использованием PSK устройства «видят» все передаваемые пакеты, и злоумышленнику не составит особого труда после успешного подключения просматривать весь трафик, идущий через точку доступа. Здесь есть технические трудности, но они достаточно легко решаются, если взломщик знает ключ PSK. Возможные риски в данном случае – не только нарушение работы системы, но и хищение персональных данных или данных о функционировании системы и идентификации пользователей, что может повлечь гораздо более серьёзные последствия.

Другой режим работы WPA2 – Enterprise, используется, как правило, в корпоративных сетях, где защите информации и управлению доступом уделяется гораздо больше внимания. Суть этого режима в том, что устройство при подключении к точке доступа проходит авторизацию на специально выделенном сервере, который даёт точке доступа разрешение на подключение (см. рис. 1). Этот процесс может происходить по комбинации логина и пароля, либо при помощи сертификата безопасности, предоставляемым тем же сервером или доверенным центром сертификации. Преимущество данного метода в том, что каждый пользователь имеет свой уникальный идентификатор для авторизации, а во время работы использует уникальный ключ шифрования. Поэтому, даже

если одно устройство будет скомпрометировано, достаточно просто поменять параметры авторизации данного устройства либо исключить его из базы данных сети. При этом работоспособность всей системы может и не пострадать вовсе (при условии достаточного резервирования её функциональности). Кроме того, в сети с таким режимом работы будет невозможно прослушивать трафик других устройств. Ещё одним преимуществом применения защиты с использованием протоколов Enterprise является возможность по уникальному идентификатору разграничивать доступ клиентов к ресурсам сети. Например, на одной точке доступа можно будет создать несколько сетей, которые хоть и будут использовать один и тот же SSID, но в соответствии с политиками доступа, определёнными на сервере, будут иметь возможность работать только с теми ресурсами, к которым им разрешено подключаться. В случае с PSK для того, чтобы реализовать аналогичное разграничение прав, необходимо установить несколько точек доступа с разными SSID.

Недостатком режима Enterprise является необходимость приобретения и установки RADIUS-сервера, но эти затраты с лихвой окупаются высоким уровнем безопасности системы и минимизацией возможных рисков.

Безопасность коммуникационного канала

Мы рассмотрели, каким образом можно подключиться к точке доступа. Теперь, когда подключение установлено, можно осуществлять передачу данных. Какие здесь существуют подводные камни?

Если сеть является закрытой, т.е. не имеет выхода в Интернет, то, в принципе, можно сосредоточиться на защите доступа к этой сети. Однако как только вы организуете канал для связи с внешним миром или даже другой сетью, у которой есть выход в Интернет, нужно будет позаботиться о защите канала связи. Говоря о защищённом канале, мы предполагаем, что реализовано следующее:

- взаимная аутентификация клиента и веб-сервера, к которому происходит обращение (иногда это сочетается с проверкой прав доступа). Как правило, такая аутентификация реализуется с помощью сертификатов с цифровой подписью (алгоритм RSA);
- осуществляется проверка целостности данных (проверка контрольных сумм и хэшей данных, например, при помощи алгоритмов MD5, SHA-1, SHA-2);
- шифрование с помощью уникальных ключей (алгоритмы AES, DES, 3DES).

Только при реализации этих трёх пунктов соединение можно считать защищённым для передачи по нему значимой информации. Это и является главной проблемой, т.к. полное выполнение перечисленных условий требует либо значительной вычислительной мощности, либо аппаратного ускорителя шифрования, либо и того, и другого. Встраиваемые системы, как правило, большой вычислительной мощностью не обладают – обычный датчик может быть реализован даже на 8-разрядном микроконтроллере. А аппаратное шифрование увеличивает их стоимость. Таким образом, дешёвые Wi-Fi-модули не предоставляют никаких возможностей ни для аутентификации, ни для проверки целостности данных, ни для их шифрования. Конечно, можно использовать внешний микроконтроллер, который будет выполнять эти функции, а Wi-Fi-модуль будет использоваться практически как модем. Но тогда теряется главный их козырь – цена, а озвученные ранее недостатки остаются не устранёнными. Кроме того, в погоне за дешевизной аппаратного решения разработчики реализуют не весь функционал для защиты канала связи, оставляя, тем самым, лазейки для хакеров.

Многие разработчики уповают на то, что они передают данные по открытому каналу уже в зашифрованном виде, например, используя VPN. Поэтому, казалось бы, можно не беспокоиться о дополнительных мерах безопасности. Но при отсутствии взаимной аутентификации клиента и сервера это теряет смысл, поскольку в таком случае невозможно гарантировать, что пакет, переданный серверу А от клиента Б, действительно передан от клиента Б, а обратный отклик от сервера А клиенту Б действительно приходит от сервера А. На этом строится основная масса атак типа «человек посередине», когда процесс авторизации клиента и сервера перехватывается, и дальнейшее общение между ними идёт уже через третий сервер, который будет использоваться злоумышленниками для перехвата данных, передаваемых по якобы защищённому каналу. Вычислив на основе перехваченных данных сессионные ключи, можно будет расшифровать весь трафик, идущий по каналу. Поэтому пользоваться открытым каналом можно лишь будучи уверенным в аутентичности реципиентов.

Как правило, в большинстве систем общение с внешними сервисами происходит на уровне HTTP-протокола (с применением методов типа POST или GET, реализованные в частности, в RESTful API) поверх TCP или в форме событийно-управляемого обмена (такой вид коммуникации поддерживается в протоколах типа MQTT или CoAP) с использованием UDP для уменьшения времени реакции или снижения нагрузки на сеть. Если не применять дополнительных мер, то вся информация будет передаваться в открытом виде и создаст условия для утечки данных или несанкционированного проникновения в систему.

Согласно статистике, примерно 20% всех утечек данных в сети и взломов в 2015 г. произошло именно из-за недостаточной защиты транспортного уровня. Единственный способ борьбы с перехватами сессий, атаками типа «человек посередине» и другими подобными методами – полная реализация SSL/TLS-протоколов и их использование при каждом обращении клиента к серверу, аутентификация с помощью сертификатов с цифровой подписью и контроль целостности данных.

Функциональная безопасность и защита интеллектуальной собственности

Важным элементом защиты беспроводных систем является обеспечение функциональности устройства в случае каких-либо сбоев. Конечно, все возможные сценарии рассмотреть сложно, но остановимся на некоторых основных моментах:

- поведение устройства в случае пропадания соединения с сетью;
- обслуживание устройства – его установка, настройка, конфигурация и обновление ПО.

Почему важно продумать поведение устройства при пропадании связи? Рассмотрим пример: у нас есть устройство, которое регулирует подачу воды в ванну или любую другую ёмкость. Сигнал о начале или прекращении подачи воды устройство получает через сеть Wi-Fi от датчика уровня. Предположим, что мы получили сигнал о том,

что уровень жидкости снизился, соответственно, мы открываем кран подачи воды и ждём сигнала о том, что вода достигла нужного уровня. Если в этот момент пропадёт соединение с сетью и, соответственно, связи между датчиками не будет, то вполне возможно, что кран так и не будет закрыт, что приведёт к затоплению помещения. Возможным выходом из ситуации будет реализация алгоритма, по которому в случае обрыва соединения кран будет автоматически закрываться. Подобные задачи решаются алгоритмически. Достаточно написать код, отладить его и прошить в готовое устройство. На первый взгляд, сложностей тут никаких нет, но при использовании нестандартных синтезируемых ядер написание программного кода и его отладка могут превратиться в нетривиальную задачу. Поэтому намного удобнее использовать стандартные процессорные ядра, для которых существуют проверенные и отработанные инструментальные средства.

Гораздо интереснее дело обстоит с обслуживанием устройств, начиная с момента их установки на объекте и на протяжении всего срока службы. На что здесь стоит обратить внимание с точки зрения обеспечения безопасности?

При подключении к сети на устройстве появляется её профиль, включающий помимо SSID также пароль для подключения или сертификат для аутентификации на RADIUS-сервере. Как правило, этот профиль сохраняется во внешней памяти, в качестве которой используется флэш-память, подключаемая по SPI. Здесь нас может поджидать первый сюрприз: на многих Wi-Fi-модулях, особенно китайских, содержимое flash-памяти никак не шифруется. Поэтому процесс взлома сети может заключаться в том, что с объекта похищается одно из устройств (либо злоумышленник каким-то образом получает физический доступ к нему), из которого извлекается микросхема памяти и считывается пароль сети. Если учесть, что там же может храниться и пользовательский код, то и он станет известен взломщику. Второй сюрприз состоит в том, что в подобных системах зачастую отсутствует привязка микросхемы памяти к микросхеме Wi-Fi-контроллера, а если даже привязка и есть, то при анализе пользовательского кода её можно легко вычислить и обойти. Это позволит злоумышленникам просто скопировать устройство и наладить выпуск аналогичного, с минимальными затратами на разработку. Защититься от копирования кода можно только путём использования внешнего контроллера, что ведёт к удорожанию системы. Однако с хранением Wi-Fi-профилей сетей без шифрования содержимого flash-памяти, увы, ничего сделать нельзя.

С аппаратной точки зрения обезопасить себя от подобных атак можно посредством использования защищённого специализированного загрузчика, прошитого в ПЗУ Wi-Fi-контроллера, который может шифровать и дешифровать данные при записи или чтении из внешней памяти. С его помощью можно также осуществить однозначную привязку микросхем друг к другу – одно без другого работать не будет, поэтому реверс-инжиниринг будет весьма затруднён и фактически потеряет смысл.

Другой, не менее важный аспект обслуживания устройства – обновление ПО в устройстве. Этот механизм

Таблица 1. Перечень наиболее распространённых угроз

Угроза	Описание	Последствия
Удалённый взлом	Несанкционированный доступ к устройству и его данным, полный или частичный. Производится по сети	Нарушение внешней безопасности устройства, утечка данных
Локальный взлом	Несанкционированный доступ к устройству и его данным, полный или частичный. Производится при помощи локального подключения к устройству с помощью аппаратных и программных средств	Нарушение безопасности устройства, утечка данных
Изменение прав доступа	Изменение прав доступа для несанкционированного доступа к защищённым ресурсам	Сбой или снижение уровня защиты устройства расширяет уровень доступа к ресурсам устройства или системы на постоянной или временной основе
Подмена	Оригинальный ресурс (сервер или клиент) подменяется ложным	Сбой или снижение уровня защиты устройства расширяет уровень доступа к ресурсам устройства или системы на постоянной или временной основе
Получение постоянного доступа к устройству	Постоянный доступ после взлома, получаемый при помощи изменения конфигурации, модификации ПО или других программно-аппаратных манипуляций	Система безопасности уже не обеспечивает нормального уровня защиты, меры по её усилению неэффективны
Отказ в обслуживании	Полное или частичное нарушение функциональности на временной или постоянной основе	Снижение или нарушение доступности сервисов, предоставляемых системой или устройством
Перехват или модификация трафика	Передаваемые по сети данные перехватываются или модифицируются	Аутентичность и сохранность данных, передаваемых по сети, больше не могут быть гарантированы
Доступ к запоминающим устройствам	Чтение или модификация данных, хранящихся на устройстве	Аутентичность и сохранность данных, хранящихся на устройстве, больше не могут быть гарантированы

необходим для внедрения новых функциональных возможностей, а также для исправления ошибок. В последнем случае мы имеем дело не только с пользовательским кодом, но, зачастую, и со стеками протоколов, которые прошиты в ПЗУ Wi-Fi-контроллера. В современном мире нередки случаи, когда в том или ином протоколе находят различные уязвимости или ошибки, поэтому для обеспечения максимального уровня защиты нужно обязательно предусматривать какой-либо вариант для обновления ПО. Наиболее распространённым способом является обновление «по воздуху» (Over-the-Air, OTA). Несмотря на то, что такие механизмы уже давно разработаны и реализованы, сложности, тем не менее, возникают. Во-первых, для передачи обновления требуется организация защищённого канала связи, иначе в момент обновления злоумышленник может провести атаку с перехватом сессии и вместо оригинального файла новой прошивки передать вредоносный код. В результате он получит контроль над устройством и сможет получить доступ к данным, передаваемым в сети. Во-вторых, необходимо предусмотреть возможность отмены обновления. Например, в результате сбоя передачи новая прошивка может быть повреждена и после того, как она будет запрограммирована в устройство, последнее может превратиться, как говорят, в «кирпич». Это может произойти и при отключении питания в момент программирования нового ПО. В связи с этим необходимы механизмы проверки правильности и подлинности прошивки, наряду с реализацией защиты от сбоев в процессе записи в ПЗУ.

Анализ рисков

При разработке встраиваемых систем важно не просто реализовать беспроводное соединение, но и сделать его максимально безопасным. С увеличением количества устройств, подключённых к сети, возрастает и количество потенциальных точек взлома. Необходим тщательный анализ возможных угроз и связанных с ними рисков, как для самой системы, так и для её пользователей. К сожалению, на данный момент нет никаких чётких руководств или стандартов, описывающих средства и меры организации защиты для технологий IoT и вряд ли можно ожидать их появления в ближайшее время. Тем не менее, есть ряд организаций, в том числе и некоммерческих, которые пытаются структурировать уязвимости и выработать определённые рекомендации по разработке встраиваемых систем для работы в облачных сервисах. Одна из таких организаций – OWASP (Open Web Application Security Project) [5] – в рамках проекта по безопасности IoT проводит постоянный анализ возможных атак и уязвимостей для подключаемых к Интернету устройств и их ПО. Для разработчиков этот проект может быть интересен тем, что указывает возможные точки атак и слабые места, которые могут сделать атаку успешной, и, что особенно важно, также предоставляет рекомендации по обеспечению безопасности как для разработчиков устройств, так и для тех, кто предоставляет облачные сервисы. Анализ возможных рисков и их последствий должен являться непременной частью любой разработки, чтобы инженер мог чётко себе представлять, какой комплекс аппаратных и программных средств ему нужно реализовать. В качестве отправной точки можно использовать данные из таблицы 1.

При разработке устройств с беспроводным подключением (в том числе по Wi-Fi), важно осознавать, что устройство само по себе – только часть системы, которая, в свою очередь, может являться элементом более крупной структуры. Если центральные узлы, как правило, располагаются в местах с контролируемым доступом, то оконечные узлы часто находятся там, где доступ к ним контролировать сложно или невозможно. Поэтому даже при реализации всех мер безопасности нельзя гарантировать, что со временем какое-то из устройств не будет скомпрометировано (например, украдено с целью реверс-инжиниринга). Разработчику уже на стадии дизайна нужно учитывать эту ситуацию и продумывать обеспечение безопасности на более высоком уровне – то, как вся система будет функционировать в условиях, когда одно или несколько устройств окажутся взломанными. Также необходимо иметь возможность своевременного и быстрого обновления ПО в случае обнаружения каких-либо уязвимостей или ошибок в программном коде.

Рекомендации по выбору элементной базы

После анализа возможных рисков можно определиться с подбором аппаратной части для решения технической задачи. Компания Texas Instruments предлагает линейку различных решений для реализации Wi-Fi-соединений. Это как отдельные микросхемы, так и готовые сертифицированные модули. Наиболее интересно с точки зрения доступности семейство SimpleLink, в которое входят две серии устройств: CC31xx и CC32xx. Первая представляет собой сетевой процессор (NWP), во вторую помимо NWP интегрированы процессорное ядро и различные периферийные модули (см. рис. 2). Основное отличие этих продуктов от дешёвых китайских аналогов – гораздо более высокий уровень защиты на всех трёх уровнях: безопасность Wi-Fi-подключения, защищённость коммуникационного канала и наличие аппаратных средств для обеспечения функциональной безопасности. В таблице 2 приведено краткое сравнение CC31xx и CC32xx с одним из китайских продуктов (Производитель А). Как можно видеть из таблицы, китайский производитель предлагает более слабый уровень защиты, сохраняя важную информацию (пользовательский код и сертификаты аутентификации) в открытом виде, а также не обеспечивая защиту процесса обновления прошивки. Однако реализация крупных проектов масштаба предприятия или проектов с повышенными требованиями к безопасности требует более защищённых решений. Компания Texas Instruments уделяет большое внимание обеспечению безопасности решений на базе семейства SimpleLink. В начале 2017 г. ожидается появление следующего поколения этих устройств, где будет реализована защищённая загрузка, расширится набор алгоритмов шифрования и появятся новые функциональные возможности для обеспечения более надёжной защиты пользовательских данных.

С точки зрения информационной безопасности, технологии, лежащие в основе IoT, уже достаточно давно и хорошо изучены. Основная сложность состоит в том, что раньше они использовались в компьютерных сетях, а теперь переносятся на встраиваемые устройства, которые не обладают аналогичной вычислительной мощностью. Поэтому велик соблазн упростить защиту или вовсе отказаться от неё. Казалось бы, кому и зачем может понадобиться взламывать бытовой или промышленный прибор? Однако вместе с расширением возможностей, которые нам открывает мир подключённых к беспроводной сети приборов, в равной степени растёт и количество угроз со стороны незащищённых устройств, при этом их опасность зачастую даже трудно себе представить. Просто вдумайтесь в эту цифру – миллиарды устройств в сети уже через несколько лет! Если обеспечению их безопасности не будет уделяться должного внимания, то мы можем оказаться в очень тяжёлой ситуации. Самое время задуматься о безопасном Интернете вещей, особенно если вы сами являетесь их разработчиком.

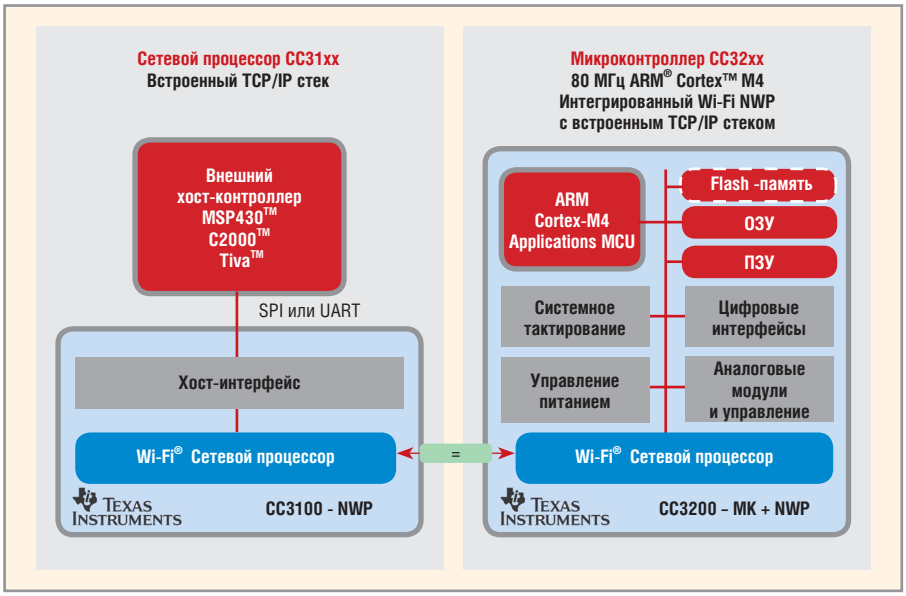

Рис. 2. Внутренняя структура CC31xx и CC32xx

Таблица 2. Сравнение параметров безопасности беспроводных компонентов

Параметры	CC31xx	CC32xx	Производитель А
Безопасность Wi-Fi			
Personal Security	ДА	Да	Да
Enterprise Security	ДА	Да	Нет*
Безопасность канала связи			
Алгоритмы	SSL3.0 TLS 1.2 X.509 AES256 3DES MD5 SHA2 RSA ECC	SSL3.0 TLS 1.2 X.509 AES256 3DES MD5 SHA2 RSA ECC	Нет*
Функциональная безопасность			
Хранение Wi-Fi-профиля	Зашифрован	Зашифрован	В открытом виде
Хранение сертификатов	Зашифрован	Зашифрован	В открытом виде
Возможность OTA	Да	Да	Да**
Программирование	Нет (внешний микроконтроллер)	Да (Cortex-M4)	Да (Tensilica Core или внешний микроконтроллер)

** Возможно с помощью внешнего процессора.*

*** Загрузка образа по незащищённому каналу в открытом виде.*

Литература

1. www.money.cnn.com/2015/07/24/technology/chrysler-hack-recall.
2. www.blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained/9493.
3. www.cnet.com/how-to/what-is-a-ddos-attack.
4. www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806.
5. www.owasp.org/index.php/OWASP_Internet_of_Things_Project.