ПРОЕКТИРОВАНИЕ ОТКАЗОУСТОЙЧИВЫХ, НАДЕЖНЫХ И ЗАЩИЩЕННЫХ СИСТЕМ ДЛЯ ИНТЕРНЕТА ВЕЩЕЙ

ЯН ПИРСОН (IAN PEARSON), Microchip Technology

Разработка и проектирование встраиваемых систем претерпела изменения с появлением технологии IoT, которая подразумевает подключение каждого встраиваемого устройства к интернету. От системы и ее узлов ожидают соответствия современным тенденциям, должного уровня безопасности и при этом – простоты обновления на уровне приложений для персонального компьютера. Несмотря на кажущуюся сложность проектирования такой системы, при правильном подходе оно не составит особых проблем.

При создании встраиваемой системы интернета вещей необходимо учитывать особенности разработки и роль каждого конкретного устройства в данной системе, проводя моделирование угроз и анализ рисков. Независимо от типа подключения к сети (проводной или беспроводной) срок службы устройства может составлять 1–20 лет, в течение которого оно может подвергнуться атаке. Именно поэтому безопасность является ключевым параметром при проектировании системы, который подразумевает возможность защищенного выполнения всего алгоритма устройства, а также его обновление.

Как следствие, с самого начала разработки системы или устройства следует учитывать, какое подключение к интернету будет использоваться, как станет выглядеть архитектура системы, что будет собой представлять процесс управления событиями, а также алгоритмы по решению возможных проблем, неминуемо возникающих, например, при расширении сети.

Поскольку разработка серийного IoT-устройства сопряжена со множеством аспектов, в т. ч. с процессами взаимодействия с отделами информационных технологий, маркетинга, инженерными подразделениями, отделом продаж, исполнительным персоналом, финансистами, юристами и т. д., следует заранее учесть все тонкости работы, стоимость и возможности устройства. Кроме того, следует учесть вопросы соответствия существующим стандартам.

К этим вопросам, в частности, относится соответствие изделия предъявляемым требованиям, алгоритмы сбора, хранения и обработки данных, а также способы устранения неполадок и нарушения целостности хранилища данных. Кроме того, необходимо построить бизнес-модель для расчета долгосрочных затрат на эксплуатацию устройства и обслуживание облачных хранилищ, если такие имеются. Работоспособность изделия и его поддержка в течение продолжительного промежутка времени зависит от правильного анализа этих исходных вопросов.

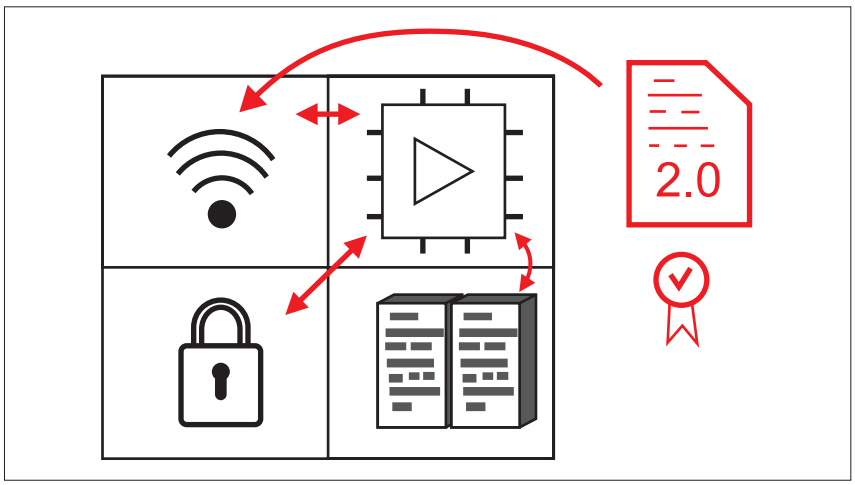

Рис. 1. **Основные элементы IoT-устройства**

Вопросы соответствия стандартам постоянно усложняются с появлением нового законодательства. Простоту использования и соответствие стандартам безопасности часто трудно сочетать в одном устройстве, а внедрение паролей и регистрации в сети не всегда просто организовать, не усложнив интерфейс. Равновесие между безопасностью и простотой, а также четкий план проектирования является залогом успешного создания устройства интернета вещей.

Основу работы подключенного к сети устройства (см. рис. 1) составляют несколько основных элементов:

- элемент обработки данных;
- элемент памяти;
- элемент коммуникации;
- безопасный аппаратный элемент;
- программное обеспечение.

Эти элементы – общие для всех решений IoT, однако принцип их реализации является индивидуальным, зависит от дизайна и особенностей проектирования устройства, а также от оценки рисков, стоимости, функций, безопасности и ремонтопригодности.

Конечной целью является разработка надежной, отказоустойчивой,

безопасной, масштабируемой, простой в обслуживании и в использовании технологичной системы, способной восстанавливаться. Кроме того, она должна обладать целостностью и иметь приемлемый уровень затрат не только на производство устройств, но и на их последующее обслуживание. Схематичный пример такого решения приведен на рисунке 2.

Заметим, что затраты на проектирование, разработку и изготовление подключаемого к интернету устройства больше, чем на устройство, работающее в автономном режиме и не способное к обновлению «по воздуху». Однако при правильном подходе к проектированию ценность подключаемого к беспроводной сети устройства в долгосрочной перспективе намного превышает стоимость компонентов и затраты на разработку. Намного разумнее и выгоднее корректно разработать IoT-систему на начальном этапе, а не пытаться что-то исправить в ней уже потом, когда что-то пойдет не так.

В некоторых ситуациях устройства интернета вещей могут использовать более одного процессора, особенно если им необходимо обрабатывать информацию, полученную через протоколы Wi-Fi, Bluetooth и т. д. Точная архитектура системы зависит от варианта ее использования, потребностей, рисков и других факторов.

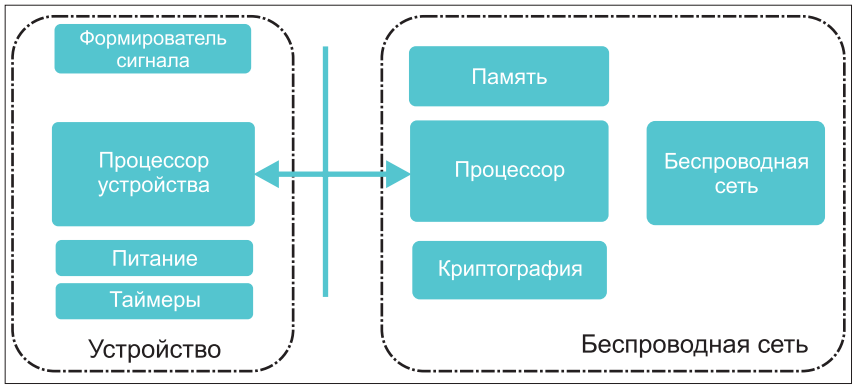

Рис. 2. **Пример беспроводного решения**

КОРЕНЬ ДОВЕРИЯ

Безопасная система требует надежных средств для хранения информации и проверки подлинности запросов; при этом гарантируется, что защищенные данные никогда не будут утеряны. Т. н. «якорь доверия» (trust anchor), являющийся по своей сути некоторым защитным элементом, отвечает именно за это. Данные элементы обеспечивают несколько методов для предотвращения аппаратных атак, добавляя в устройство такие функции как генераторы случайных чисел (Random Number Generators, RNG), соответствующие NIST SP 800 и криптографические алгоритмы, например FIPS, совместимые с ECDSA-P256 (Elliptic Curve Digital Signature Algorithm – алгоритм цифровой подписи на эллиптической кривой).

Перечислим функционал, который обеспечивают защитные элементы.

- Аутентификация устройства в облачных сервисах с использованием протестированных и понятных методологий инфраструктуры открытых ключей (public key infrastructure, PKI). Аутентификация позволяет осуществлять предварительную регистрацию устройств в системе и выдавать каждому из них при изготовлении индивидуальный сертификат, а также генерировать QR-код, служащий для связки конечного изделия с сертификатом. Полученный QR-код пользователь привязывает к своей учетной записи при вводе устройства в эксплуатацию.

Компания Microchip Technology недавно представила первое в отрасли предварительно подготовленное решение для безопасного ключа. Оно упрощает создание автоматизированной системы безопасной аутентификации для проектов практически любого объема. Данная трехуровневая система, известная как платформа доверия (Trust Platform), предоставляет готовые предварительно настроенные или настраиваемые защитные элементы и встраивается для аутентификации в любой инфраструктуре публичной или частной сети, в т. ч. сети LoRaWAN.

- Аутентификация данных. С ее помощью можно определить, были ли данные получены с конкретного устройства и не были ли они подменены в процессе передачи. Аутентификация позволяет обнаруживать аномалии в данных с помощью облачной аналитики.
- Безопасная загрузка. Это использование закрытого алгоритма, хранящегося в элементе безопасности, для идентификации изменений в криптографической подписи главного МК и сохраненных образов обновления прошивки. Кроме того, используются дополнительные проверки целостности с помощью методов из библиотек безопасности класса B (Class B Safety Libraries).
- Безопасное обновление встроенного программного обеспечения по беспроводной сети (Secure Firmware Upgrade Over the Air, FUOTA): алгоритм, хранящийся в элементе безопасности, используется для проверки источника обновления, а также подписи образа, отправляемого на устройство для подтверждения его корректности до начала загрузки обновления.
- Защита от клонирования. При правильном использовании защитный элемент позволяет предотвратить клонирование и подделку оборудования.

Однако наличие и корректное использование защитных элементов подразумевает, что устройства были первоначально запрограммированы в безопасной производственной среде. Данный аспект создает проблемы, связанные с масштабируемостью производства, особенно в тех случаях, когда в производственную цепочку приходится включать подрядчиков и субподрядчиков. Гибкость производства, простой ввод в эксплуатацию, а также наличие защитных алгоритмов не только на предприятии, но и в самом устройстве позволяют конечному пользователю получить надежное устройство с возможностью безопасного подключения к сети и обновления.

ОБНОВЛЕНИЕ И ПАМЯТЬ

Традиционно обновление прошивки устройства выполняется при помощи кабеля, подключаемого напрямую к устройству через последовательный порт. Такой подход использовался много лет, но он малопригоден для крупных масштабируемых сетей с множеством устройств, которые, кроме того, могут быть труднодоступными для такого типа подключений.

В случае возникновения необходимости незапланированного обновления следует избегать подхода, требующего физического вмешательства. Альтернативой проводного подключения является использование обновлений при помощи FUOTA и, предпочтительно, безопасных FUOTA. Кроме того, на практике система должна использовать преимущества элементов безопасности, интегрированных в каждое устройство, чтобы предотвратить несанкционированные действия и обновления от неизвестных или ненадежных источников.

Но как правильно осуществить процесс обновления? В идеале, безопасный процесс обновления при помощи FUOTA должен выполняться, не затрагивая алгоритм, который выполняется в микроконтроллере. Запись файла обновления непосредственно на флэш-память устройства без создания локальной резервной копии прошивки порождает риск превращения устройства в «кирпич» в случае возникновения в процессе обновления критической ошибки.

Интерфейс сети обновления по FUOTA должен иметь достаточную пропускную способность для продолжения процесса обновления в случае возникновения задержек, отключений или ошибок. Алгоритм обновления по FUOTA является наиболее гибким и легко адаптируется к сетям и конечным устройствам разных видов, чего нельзя сказать о традиционном методе, где для организации обновления могут потребоваться интерфейсы и кабели для подключения.

ПИТАНИЕ УСТРОЙСТВА И ВНЕШНИЕ ФАКТОРЫ

При развертывании сети, состоящей из множества устройств, даже при наличии алгоритма безопасного обновления нельзя в полной мере быть уверенным в отсутствии сбоев, связанных, например, с питанием и окружающими условиями, в т. ч. с электростатическими разрядами. Эти параметры также влияют на безопасность, могут заметно различаться в зависимости от каждого устройства как такового и в идеале должны учитываться при проектировании для максимального приближения рабочих характеристик в реальных условиях к лабораторным.

Взлом устройства сети может никогда не произойти на протяжении всего срока службы, что обусловлено следующими причинами и факторами.

- Простое везение. Устройство может не стать объектом интереса злоумышленника, или корректное планирование и разработка сделают задачу взлома достаточно сложной.
- Использование современных методов защиты. Хотя идеальной системы безопасности не существует и любая из них рано или поздно будет взломана, следует использовать современные методы защиты, обновляя их по мере возможности. Например, если система наделена функцией безопасного обновления, можно использовать гибкую систему защиты, централизованную в облаке.
- Применяется современный подход к разработке устройства и сети с помощью методов IoT Security Foundation, Gov.UK Secure by Design, UL2900, ISA 62443, ISA Secure и т. д.
- Система организована с учетом неизбежного увеличения размера кода.
- Исходное проектирование с учетом наихудшего сценария использования с последующим упрощением для конкретных применений, а не разработка без учета неблагоприятных сценариев. Устройства IoT имеют большой интерес для хакеров, мошенников и пользователей, желающих немного развлечься.

Причины, по которым устройство может подвергаться атаке, не имеют смысла, главное – это возможный ущерб людям, изделиям, предприятиям, брендам и компаниям, который может быть весьма значительным. Аргумент «меня это не коснется» никогда не обеспечивал надежную защиту.