«Яндекс.Облако»

и безопасность обмена данными IoT-устройств

1 октября на Yandex Scale (первая большая конференция «Яндекс.Облака») было представлено пять новых сервисов. Еще буквально в сентябре 2018 года их было лишь девять, а сейчас уже 27. В своих разработках «Яндекс» использует мировой опыт с учетом отечественных особенностей. В статье мы рассмотрим решения, имеющие непосредственное отношение к аппаратному обеспечению, а именно Yandex IoT Core и Yandex Interconnect.

Владимир Апарин, к.т.н.
vaparin@ultran.ru
Вадим Гизятулин
gvm@ultran.ru

Вопрос разработки сервиса — сложная комплексная задача, состоящая из нескольких вопросов, которые необходимо рассматривать в совокупности: функциональность, безопасность, надежность, масштабируемость, стоимость, соответствие правовым нормам и другие. Про традиционные решения для IT-сферы написано достаточно много профильными изданиями. Из последнего можно отметить, например, августовскую статью в журнале «Хакер» [1], посвященную вопросам безопасности и надежности облачных решений, начиная с уровня архитектуры. «Яндекс» продвигает современную концепцию, наиболее востребованную у разработчиков/владельцев продуктов и эксплуатирующих организаций, — предоставление сервисов без необходимости вникания в детали на всех уровнях, начиная с самого низкого. При этом с высоким качеством, надежностью, масштабируемостью и разумной стоимостью. Данной проблематике было посвящено несколько докладов от партнеров, которые уже запустили свои решения в облаке, ознакомиться с материалами можно в [2]. Мы же рассмотрим варианты, наиболее близкие разработчикам аппаратных решений, которые одновременно являются новыми для «Яндекса».

Yandex IoT Core [3] — группа решений, оптимизированных для «Интернета вещей». Включает MQTT-брокер, интерфейс для группового управления устройствами и, конечно, простую интеграцию с остальными сервисами «Яндекс. Облака».

При разработке IoT Core «Яндекс» использовал опыт мировых лидеров среди поставщиков облачных сервисов: «большой тройки» AWS, Google Cloud, Microsoft Azure и набирающей обороты Alibaba Cloud, и тем самым уже с самого начала заложил наиболее современные и актуальные решения. В текущий момент доступно два интерфейса консоли: командная строка на базе SH (доступна для Linux/MacOS/Windows) и веб. Оба варианта позволяют добавлять устройства, группы, подписывать SSL-ключами и генерировать уникальные топики.

Следует отметить, что практически все компании — производители электроники в РФ не хотят или не имеют возможности поддерживать собственную IT-инфраструктуру, особенно на этапе роста, когда требуется обеспечить стабильность и масштабируемость решения, а также его надежность и отказоустойчивость. В то же время, когда продукт вышел на стадию стабильного оборота и большого числа клиентов, менять что-либо в инфраструктуре крайне сложно и ресурсозатратно. А зачастую просто невозможно, поэтому необходимо выбрать правильное решение уже на этапе проработки архитектуры. Учитывая опыт, квалификацию и ресурсы компании «Яндекс», в предлагаемых решениях можно не сомневаться и избавить себя от реализации непрофильных проблем.

С этой точки зрения решения «Яндекса» выглядят очень интересными.

Рассмотрим основные ключевые особенности Yandex IoT Core.

- Обеспечение мировых стандартов безопасности на отечественной платформе:
  - TLS/SSL-шифрование;
  - каждое устройство и реестр имеет свой ключ;
  - уникальные идентификаторы топиков для каждого устройства;

  - собственная реализация MQTT-брокера, оптимизированная под безопасность.
- Гибкий подход к решаемой задаче:
  - группировка устройств;
  - различные характеристики ключей (длина, версии TLS);
  - масштабируемость и резервируемость решения;
  - удобные тарифные планы (как на этапе запуска, так и при масштабировании).
- Техническая поддержка на русском языке.
- Хранение данных на территории РФ:
  - соответствие законам Яровой о хранении данных;
  - возможность участия в гостендерах;
  - малые задержки из-за близости расположения и работе с провайдерами.

Среди успешных примеров применения Yandex IoT Core можно назвать:

- онлайн-кассы компании «Мультисофт»;
- систему сбора и учета энергоресурсов от компаний из Санкт-Петербурга Red Bees и SayMon.

Онлайн-кассы компании «Мультисофт» занимают второе место среди онлайн-касс в РФ. С точки зрения техники решение построено на базе OEM-дизайна POS-терминала на ОС Android. «Мультисофт» реализовал свою прошивку с необходимыми функциями. Интеграция с сервисами «Яндекса» позволила получить анализ функционирования оборудования для предсказания выхода из строя, а также удаленного обновления. Тем самым значительно снижены затраты на поддержку оборудования в рабочем состоянии. Это особо актуально для онлайн-касс, поскольку с 2018 года все покупки должны проходить через них, а при выходе кассы из строя работа торговой точки может быть парализована, что приводит к прямым убыткам.

Устройство сбора и передачи данных (УСПД) относится к классу устройств, которые появились пару лет назад и набирают все большую популярность на рынке РФ. С технической точки зрения УСПД являются развитием класса модемов за счет добавления функций автоматического автономного опроса конечных устройств (счетчиков, вендинговых аппаратов и др.) и последующей передачи данных на сервер (рис.). Тенденция снижения энергопотребления и расходов на сотовую связь дает ряд преимуществ.

Особо следует отметить, что представленное на конференции УСПД реализовано на базе технологии NB-IoT, которая также активно развивается последний год, с тех пор как операторы заявили о коммерческом запуске сетей нового поколения, и которая тоже ориентирована на снижение трафика и тока. Вопрос безопасности NB-IoT стоит рассмотреть отдельно, так как, к сожалению, он находится на граничной области между аппаратной и программной составляющими любой платформы и ему зачастую уделяют не так много внимания.

Например, практически все современные облачные сервисы («большой облачной тройки» и «Яндекс») требуют поддержки шифрования TLS, поскольку это соответствует мировым тенденциям в области безопасности со стороны IT. Однако в то же время производители модулей NB-IoT лишь заявляют поддержку TLS/SSL, но не осуществляют ее на практике. Или же она сильно ограничена и не позволяет использовать решение в должной мере. К сожалению, такова реальная ситуация, с которой столкнулись разработчики Red Bees при интеграции УСПД с Yandex IoT Core.

Был проведен анализ доступных на российском рынке модулей NB-IoT (всего восемь производителей) на предмет поддержки MQTT TLS. Реальная поддержка TLS over NB-IoT была лишь у двух производителей модулей сотовой связи, доступных на отечественном рынке, — Nordic Semiconductor (nRF9160) и uBlox (SARA-R410). Первые использовали TLS из Zephyr OS, на базе которой работает SIP, вторые реализовали собственный стек, управляемый AT-командами.

Дешевые модули NB-IoT со значительной долей вероятности не смогут реализовать поддержку MQTT и TLS из-за ограниченности ресурсов и по этой причине останутся вне рынка, обеспечивающего безопасность. В то же время для более производительных модулей NB-IoT поддержка TLS является вопросом времени и приоритета со стороны отдела разработки ПО производителя. В текущий момент такой функционал доступен лишь у лидеров рынка, уделяющих много внимания качеству ПО и безопасности.

Есть мнение, что TLS и MQTT не являются необходимыми для IoT-продуктов. Обычно это аргументируется тем, что применение данных технологий приводит к дополнительным затратам с точки зрения трафика в первую очередь и вычислительных ресурсов во вторую и, как следствие, к повышенному энергопотреблению. Это действительно так, однако в данных рассуждениях не анализируются проблемы безопасности и надежности в принципе. Необходимо рассмотреть вопрос более подробно на всех уровнях. Использование UDP не дает гарантии доставки сообщения, а доработка протокола для получения подтверждения не несет особого выигрыша относительно TCP, при этом появляется потенциальная уязвимость и точка отказа. Пара ключ/пароль для MQTT не достаточна для обеспечения безопасности как минимум потому, что данные передаются в открытом виде (их можно перехватить и подменить впоследствии). А также ее можно подобрать за время жизни устройства (в большинстве случаев после установки настройки на нем не меняются вообще). Кроме того, можно подменить сам сервер на принимающей стороне, и без TLS конечный пользователь так и не узнает, что данные передает «не туда». Использование только TLS-сокета без высокоуровневого протокола (например, MQTT или подобного) потребует собственной реализации сервера для сбора и хранения данных с множества устройств, а тут уже опять возникают вопросы надежности и масштабируемости. В итоге по-

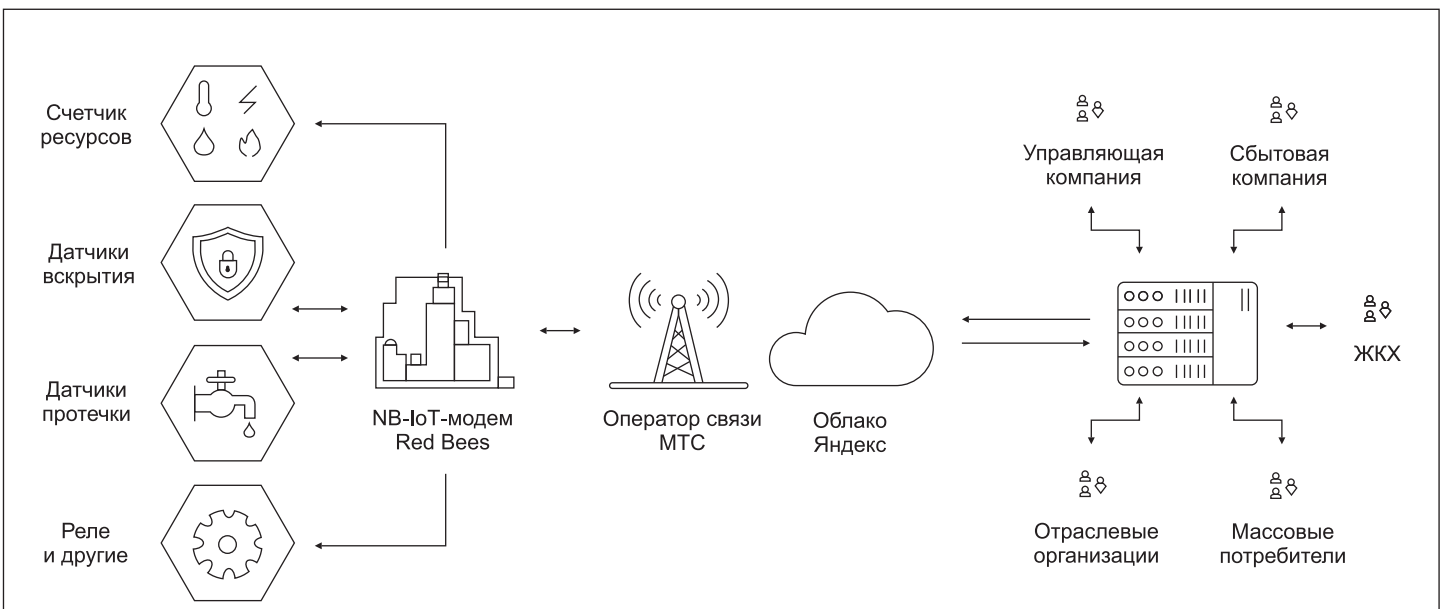

Рис. Типовое решение для сбора и передачи данных на базе NB-IoT

лучается изобретение велосипедов, вместо того чтобы запустить продукт в серию и получать прибыль. Мысль об отсутствии необходимости MQTT и TLS пока достаточно распространена среди тех, кто начинает осваивать «Интернет вещей» и кто пока не столкнулся с проблемами безопасности.

Yandex Interconnect [4] объединяет провайдеров и дата-центры. Целью является соединение всех операторов связи в общую структуру для минимизации задержек передачи данных между инфраструктурой конечного пользователя и практически всеми публичными облаками.

Основой решения Yandex Cloud Interconnect служит магистральный канал (транк-соединение) с пропускной способностью 100 Мбит/с — 10 Гбит/с и более. Поверх магистрального канала создаются выделенные приватные соединения. Управление осуществляется аналогичным образом — через консоль. В текущий момент партнерами данного сервиса являются пять операторов связи, и их количество увеличивается. Подобный подход позволяет пользователю также не заботиться о конкретных вопросах реализации и получить конечный сервис.

В заключение следует отметить, что представленные в октябре Yandex IoT Core и Yandex Cloud Interconnect являются современными облачными решениями, оптимизированными под безопасность на мировом уровне, с одной стороны, и отечественные особенности, с другой стороны. И несмотря на то, что продукт только вышел, он уже имеет позитивный опыт внедрения в РФ. Поэтому представляется возможным и интересным применение данного сервиса в отечественных разработках «Интернета вещей», так как это позволяет конечным разработчикам электроники сконцентрироваться на аспектах, в которых они являются профессионалами, а новые задачи, продиктованные современными реалиями рынка, передать партнеру, имеющему большой опыт в данном направлении. Особо интересным видится данное решение в связке Nb-IoT + TLS + MQTT, так как аналогичных продуктов от отечественных компаний на рынке нет. ■

Литература

1. www.xakep.ru/2019/08/14/yandex-cloud/
2. www.youtu.be/Jkq_byEOHIQ
3. www.cloud.yandex.ru/services/iot-core
4. www.cloud.yandex.ru/services/interconnect