ПЕРСПЕКТИВНЫЕ ВОЗМОЖНОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФРАСТРУКТУРЫ IOT

Клыбик В. П., Иванюк А. А.
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: vold029@gmail.com, ivaniuk@bsuir.by

Рассматриваются перспективы применения физически неклонируемых функций для идентификации и аутентификации устройств интернета вещей (IoT).

Введение

Интернет вещей (ИВ) (Internet of Things - IoT) — концепция, подразумевающая взаимодействие посредством сетевых коммуникаций с помощью стандартных интернет-протоколов между кибер-физическими системами, являющимися разнообразными вещами физического мира, например приборы учета электроэнергии, датчики температуры, влажности и др.

Подобные системы существовали и ранее, но ограничивались географической распределенностью, высокой стоимостью, ограниченностью коммуникаций и зонами использования. Прогресс в микроэлектронике и развитие коммуникаций привели к бурному росту количества устройств ИВ и их глубокое проникновение в различные сферы. Gartner заявляет, что в 2017 году число подключенных устройств составило 8,4 млрд [1]. Такое быстрое и широкое распространение ИВ с одной стороны дает множество новых возможностей для развития каждой сферы, с другой стороны - обостряет ряд проблем, без решения которых дальнейшее проникновение ИВ может привести к катастрофическим последствиям.

I. Инфраструктура интернета вещей

В общем случае ИВ является лишь концепцией взаимодействия посредством сетевых коммуникаций между разнообразными устройствами. Следствием для всей отрасли является высокая гетерегонность решений, отсутствие жесткой структуры, архитектуры и границ в критериях классификации.

На формирование практической инфраструктуры влияют следующие факторы:

- многие устройства ИВ крайне ограничены в вычислительных ресурсах;
- устройства общаются не только, а, иногда, и не столько между собой, сколько со специальными приложениями/сервисами, реализующими высокоуровневую сервисную логику управления или обработки полученных данных;
- прямое подключение к сети Интернет невозможно, т.к. не позволяет реализовать требования по скорости отклика/обмена, или необходимо использовать несовместимые протоколы связи.

Исходя из изложенного выше, развернутая структура ИВ представлена на Рис.1. Стрелки показывают направления управляющих и информационных потоков данных между взаимодействующими компонентами системы.

Например, компания Cisco предложила семиуровневую архитектуру ИВ[2].

II. Проблемы обеспечения целостности инфраструктуры

В любом варианте инфраструктуры совершенно важными факторами являются идентификация и аутентификация каждого компонента. Идентификация необходима в первую очередь для корректной адресации потоков управления и ассоциации данных. Аутентификация позволяет убедиться, что не произошла несанкционированная подмена компонента.

Например, в случае умного дома может быть по ошибке или злонамеренно изменена температура помещений, включена вода, свет, бытовые приборы. Как минимум, это вызовет сильный дискомфорт у человека. В случае промышленного применения ИВ последствия могут быть серьезными.

На сегодняшний день используются статический и динамический способ идентификации компонентов. Статический способ реализуется с использованием:

- прошитых идентификаторов;
- MAC-адресов;
- QR-кодов.

Динамический способ использует наблюдение и анализ сетевого трафика компонента.

В случае статического способа идентификации одной из проблем является обеспечение уникальности идентификаторов и возможность дублирования идентификаторов устройств в случае ошибки при производстве или настройке.

Динамический способ идентификации требует длительного обучения анализатора, имеет низкую стабильность и практически не применим на этапе первичного ввода компонента в эксплуатацию.

Для аутентификации устройств используются крипто-функции и крипто-протоколы, основанные на устанавливаемых на компоненты

сертификатах. Сертификат представляет собой специальный набор данных, хранимый во внутренней памяти устройства. Для успешного использования крипто-протоколов при аутентификации важными являются две проблемы:

- обеспечить неизвлекаемость сертификата из внутренней памяти устройства;
- обеспечить генерацию истинно случайных последовательностей чисел.

На сегодняшний день оба требования либо недостаточно обеспечиваются в случае массовых дешевых устройств ИВ, либо требуют применения дополнительных специализированных аппаратных решений, что ведет к удорожанию устройств [3,4].

III. Применение ФНФ

Формальное определение физически неклонируемой функции (ФНФ) цифрового устройства дано в работе [5]. Основными свойствами ФНФ являются:

- невоспроизводимость математической/алгоритмической модели;
- некопируемость при тиражировании схемной реализации.

Основными применениями ФНФ являются:

- идентификация цифровых устройств;
- генерирование крипто-ключей.

Достоинствами применениями ФНФ для ИВ является отсутствие:

- необходимости в специализированных аппаратных решениях;
- процесса назначения идентификатора устройства при производстве.

В текущее время большинство практических реализаций ФНФ основаны на программируемых логических интегральных схемах (ПЛИС), либо в составе специализированных процессоров. В случае ИВ часто используются широко распространенные микроконтроллеры. Создание реализаций ФНФ для микроконтроллеров является важной задачей для применения в ИВ. Такие ФНФ позволят повысить безопасность не только новых, но и существующих устройств ИВ, путем обновления программного обеспечения.

Выводы

С учетом роста проникновения ИВ в многие сферы жизнедеятельности человека, обеспечение безопасности становится критическим фактором успешного развития отрасли.

Применение ФНФ в задачах идентификации и аутентификации ИВ является перспективным направлением для дальнейших исследований. Необходимо как исследовать реализации ФНФ на текущем аппаратном обеспечении ИВ на предмет достаточного качества их характеристик, так и предложить реализации ФНФ в будущих версиях аппаратного обеспечения.

Литература

1. Gartner portal / Gartner Says 8.4 Billion Connected "Things"Will Be in Use in 2017, Up 31 Percent From 2016// [Electronic resource]. – Mode of access: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. – Date of access: 01.10.2018.
2. Internet of Things Word Forum / Internet of Things Word Forum[Electronic resource]. – Mode of access: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf. – Date of access: 02.10.2018.
3. State-of-the-art answers to today's embedded security challenges with OPTIGA Trust / infineon Technology portal[Electronic resource]. – Mode of access: https://www.infineon.com/cms/en/product/security-smart-card-solutions/optiga-embedded-security-solutions/optiga-trust/. – Date of access: 02.10.2018.
4. iBadge / InfoKeyVault portal[Electronic resource]. – Mode of access: http://www.ikv-tech.com/index.php/en/product/ibadge. – Date of access: 02.10.2018.
5. Ярмолик, В. Н. Физически неклонируемые функции / В. Н. Ярмолик, Ю. Г. Вашинко // Информатика. – 2011. – №2. – С. 90-100.

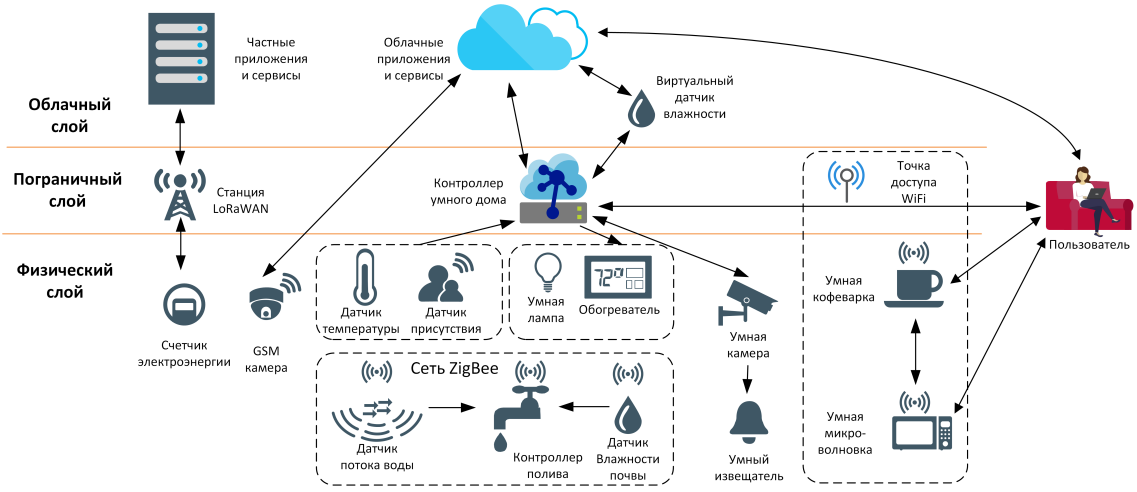

Рис. 1 – Развернутая структура системы интернета вещей