Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.77:512.624.95

Савченко
Алексей Александрович

Методика оценки параметров устройств интернета вещей при реализации ими асимметричных криптографических алгоритмов

АВТОРЕФЕРАТ
на соискание степени магистра
по специальности 1-98 80 01 Информационная безопасность

_____

Научный руководитель
Власова Галина Александровна
кандидат технических наук, доцент

_____

Минск 2021

Введение

Для большинства людей IoT – это холодильник с функцией заказа продуктов, робот пылесос, который способен пропылесосить дом, когда пользователь на работе. В мире приблизительно используется 28 миллиардов устройств, подключенных к интернету. При этом на пользовательские носимые устройства приходится менее половины всех подключенных устройств. Около 15 миллиардов устройств используют в области промышленности и бизнеса: терминалы для приема платежей банковской картой, сенсоры в общественном транспорте и т.д.

Развитие искусственного интеллекта и интернета способствуют тому, чтобы IoT считалось обязательным требованием для товаров и услуг. С разработкой миниатюрных датчиков, IoT постепенно интегрируется в тело человека. IoT делает жизнь потребителя проще. Но IoT – это устройство, подключаемое к интернету, а значит, оно уязвимо. С каждым годом атаки на интернет вещей растут с большой скоростью, так как большинство разработчиков «умных» систем относились неответственно к безопасности, например, стандартный логин и пароль от панели администрирования, а также быстрота выхода на рынок, за счет низкого порога защищенности. Или несоответствие рекламным лозунгам, о том, что в устройстве находится криптографический микроконтроллер, т.к. конфиденциальность популярна среди потребителя.

Быстрое развитие IoT и возрастающие число атак заставляет задуматься, о методики оценки параметров интернета вещей. В диссертации приводится пример реализации методики оценки параметров устройств интернета вещей при реализации ими асимметричных криптоалгоритмов.

При криптографической защите IoT устройства, криптоалгоритм «отнимает» часть ресурсов от микроконтроллера, особенно если это асимметричный криптоалгоритм. Производителю и пользователю не выгодно дополнительно нагружать вычислительное устройство, но, в последнее время, большинство потребителей все чаще начали заботиться о конфиденциальности, и готовы доплачивать. Поэтому производители стали добавлять в микроконтроллер криптографические ускорители.

В связи с этим, необходима методика оценки параметров устройств интернета вещей при реализации ими криптографического алгоритма. В диссертации исследуются, асимметричные криптографические алгоритмы, так как длина ключей и вся математика, стоящая за ними, дают достаточную гарантию того, что не существует никакого другого ключа, не являющегося частью пары, который мог бы дешифровать сообщение. В симметричных криптосистемах существует опасность раскрытия секретного ключа во время передачи.

Общая характеристика работы

Связь работы с приоритетными направлениями научной, научно-технической и инновационной деятельности

Тема диссертационной работы соответствует разделу 6 «Обеспечение безопасности человека, общества и государства» приоритетных направлений научной, научно-технической и инновационной деятельности в Республики Беларусь на 2021 – 2025 гг., утверждённых Указом Президента Республики Беларусь 7 мая 2020 г., № 156. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке методики оценки параметров устройств интернета вещей при реализации ими асимметричных криптографических алгоритмов. Для достижения поставленной цели необходимо было выполнить следующие задачи:

1 Проанализировать статистику атак и основные угрозы на устройства интернета вещей.

2 Проанализировать криптографические алгоритмы и методы их реализации для IoT устройств.

3 Разработать методику оценки параметров устройств интернета вещей при реализации ими асимметричных криптографических алгоритмов.

Апробация результатов диссертации

Основные положения и результаты диссертации публиковались в сборнике XVII Международной научно-практической конференции «Управление информационными ресурсами» (Минск, 2021).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 2 статьи в сборниках материалов конференций.

Личный вклад соискателя

Все основные результаты, изложенные в диссертационной работе, получены соискателем самостоятельно. В совместно опубликованной работе автор провел исследования по предложенной методике.

Краткое содержание работы

В первой главе, при анализе интернета вещей, стало понятно, что это необходимая и быстро развевающееся отрасль, которая привлекает злоумышленников. При быстро растущем сегментом рынка IoT вещей, многие производители пренебрегают безопасностью, поэтому необходимо создать стандарт, благодаря которому данные пользователя будут защищены. Одним из методов защиты IoT вещей является программное и программно-аппаратная реализация. При этом помочь упростить разработчикам анализ устройств и криптографических алгоритмов.

Во-второй главе, при обзоре и классификации существующих криптоалгоритмов, возникает дилемма, выбрать «быстрый», но менее защищенный малоресурсный симметричный криптоалгоритм или «медленный», но надежный асимметричный криптоалгоритм. При разработке устройств интернета вещей, разработчик для себя определяет какой криптографический алгоритм ему выбрать, исходя из специфики работы IoT устройства.

В третьей главе, была описана разработанная методика оценки устройств интернета вещей, при реализации ими асимметричных криптоалгоритмов, и даны рекомендации по ее проведению. А также даны характеристики исследуемых в апробации вычислительных устройств.

В четвертой главе, при апробации разработанной методики, очевидно, что методика работает и позволяет не только оценить эффективность микроконтроллера или центрального процессора, но и эффективность криптографического алгоритма. Рассматривался криптографический алгоритм RSA, с уровнями стойкости 128 bit, 256 bit, 512 bit и 1024 bit. В качестве вычислителей в эксперименте использовались микроконтроллеры Arduino UNO, Arduino Nano, Arduino Due, Arduino Yun, Intel Galileo, Intel Edison, STM32F103, центральные процессоры Intel i5-4590 и Intel Pentium-N3540. В результате расчета коэффициента эффективности K и K_{ws} были получены результаты, о том, что STM32F103 наиболее подходящий микроконтроллер для реализации IoT устройств.

Заключение

Интернет вещей, как любая быстроразвивающаяся технология, испытывает ряд проблем, среди которых наиболее серьезной является проблема безопасности. Чем больше «умных» устройств подключается к сети, тем выше риски, связанные с несанкционированным доступом в IoT-систему и использованием ее возможностей злоумышленниками. Сегодня усилия многих компаний и организаций в сфере IT направлены на поиск решений, которые позволят минимизировать угрозы, мешающие внедрение IoT.

В результате выполнения диссертационной работы были изучены малоресурсные криптографические алгоритмы, разработана методика оценки параметров устройств интернета вещей, при реализации ими асимметричных криптоалгоритмов, и произведена апробация.

Рассматривался криптографический алгоритм RSA, с различными уровнями стойкости. В качестве вычислителей в эксперименте использовались микроконтроллеры и центральные процессоры. В результате расчета коэффициента эффективности K и K_{ws} были получены результаты, о том, что STM32F103 наиболее подходящий микроконтроллер для реализации IoT устройств.

Методика оценки устройств, описанная в диссертации, может способствовать безопасному внедрению IoT в повседневную жизнь. На основе формул K и K_{ws} можно выбирать микроконтроллер или центральный процессор при разработке IoT, или оценивать уже существующие. Достоинством данной методики является то, что она универсальная, т.е. не привязана к алгоритмам шифрования, языку программирования и криптозащищенности. Можно исследовать как самый дешевый микроконтроллер, так и дорогой центральный процессор персонального компьютера. Так же, исходя из таблиц 18 и 19, можно сделать вывод, что методикой, описанной в диссертации, можно оценивать криптоалгоритмы, если проводить испытания на одном микроконтроллере.

Так же данная методика может быть основой для создания аппаратно-программного устройства оценки защищенности IoT. Например, с её помощью, можно написать скрипт, в котором будут данные о популярных микроконтроллерах и центральных процессоров, далее при подключении к IoT, будет производиться шифрование/дешифрования алгоритмом, который реализуется устройством по умолчанию. Результаты будут записываться в память, и пользователь, просмотрев результат, сможет оценить, подходит ли ему степень защиты IoT устройства. Данное аппаратно-программное устройство можно реализовать с помощью usb-флешки, так как почти во-всех IoT есть usb-разъем.

Публикации:

1 Савченко, А. А. Применение облегчённых криптоалгоритмов для интернета вещей / Савченко А. А., Анисимова Ю. Н. Власова Г. А. // Инфокоммуникации: сборник тезисов докладов 56-ой научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 18 – 20 мая 2020 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск: 2020. – С. 47 – 49.

2 Савченко, А. А. Оценка эффективности микроконтроллеров при реализации алгоритма шифрования RSA / Савченко А. А., Власова Г. А. // Сборник тезисов и докладов XVII Международной научно-практической конференции «Управление информационными ресурсами», 12 марта 2021 г. /

Академия управления при Президенте Республики Беларусь. –Минск: 2021 – С. 235 – 236.