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

УДК 004.056.53

Руденко
Николай Сергеевич

Методика аутентификации устройств "умного дома" на основе криптографических алгоритмов

АВТОРЕФЕРАТ
на соискание степени магистра технических наук по специальности 1-39 81 03
«Информационные радиотехнологии»

Научный руководитель

Власова Галина Александровна

Кандидат технических наук,
доцент

Минск 2018

ВВЕДЕНИЕ

Стремительное развитие микроэлектронной промышленности сделало возможным повсеместное внедрение практических решений для реализации концепции интернета вещей (IoT). Так как масштабы использования IoT постоянно растут – возникает необходимость обеспечения информационной безопасности в системах использующих такую концепцию. Однако, так как устройства, используемые в таких системах, не обладают достаточной вычислительной мощью, для их защиты необходимо использовать криптографические алгоритмы, стойкость которых снижается незначительно, в отличие от объема требуемых ресурсов, которые называются алгоритмами легковесной(lightweight) или малоресурсной криптографии.В 1985 году независимо Нилом Коблицем и Виктором Миллером было предложено использовать в криптографии алгебраические свойства эллиптических кривых. С этого момента началось бурное развитие нового направления криптографии, для которого используется термин "криптография на эллиптических кривых". Роль основной криптографической операции выполняет операция скалярного умножения точки на эллиптической кривой на данное целое число, определяемая через операции сложения и удвоения точек эллиптической кривой. Последние, в свою очередь, выполняются на основе операций сложения, умножения и инвертирования в конечном поле, над которыми рассматривается кривая. Особый интерес к криптографии эллиптических кривых обусловлен теми преимуществами, которые дает её применение в беспроводных коммуникациях — высокое быстродействие и небольшая длина ключа. Асимметричная криптография основана на сложности решения некоторых математических задач. Ранние криптосистемы с открытым ключом, такие как алгоритм RSA, криптостойки благодаря тому, что сложно разложить составное число на простые множители. При использовании алгоритмов на эллиптических кривых полагается, что не существует субэкспоненциальных алгоритмов для решения задачи дискретного логарифмирования в группах их точек. При этом порядок группы точек эллиптической кривой определяет сложность задачи. Считается, что для достижения такого же уровня криптостойкости как и в RSA, требуются группы меньших порядков, что уменьшает затраты на хранение и передачу информации. Например, на конференции RSA 2005 Агентство национальной безопасности объявило о создании “Suite B”, в котором используются исключительно алгоритмы эллиптической криптографии, причём для защиты информации, классифицируемой до “Top Secret”, используются всего лишь 384-битные ключи. Преимущества криптографии на эллиптических кривых позволяют эффективно применять её для защиты каналов связи в сетях, где устройства не обладают значительными вычислительными ресурсами. Возможно, в недалеком будущем именно эллиптическая криптография поможет решить проблему

информационной безопасности IoT устройств, поэтому она заслуживает особоговнимания. В данной статье основное внимание уделено механизмам аутентификации с использованием малоресурсной криптографии и путям их развития. В контексте этого рассмотрены некоторые уязвимости и атаки на IoT.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель данной работы: исследование методик аутентификации для систем автоматизированного жилого помещения и выявление их особенностей.

Задачи исследования: обзор подходов к эффективному использованию ограниченных вычислительных возможностей микроконтроллеров; моделирование возможных угроз информационной безопасности в системах автоматизированного жилого помещения и обозначение путей противодействия им; выбор криптографических алгоритмов для применения в микроконтроллере; выбор и адаптация ECC-библиотеки под задачи исследования; проведение сравнительных измерений параметров работы криптографических алгоритмов средствами симулятора микроконтроллера.

Объект исследования работы: особенности реализации алгоритмов аутентификации в системах «умного дома».

Предмет исследования работы: реализация эффективных алгоритмов аутентификации для защиты исполнительных устройств системы «умный дом».

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении показано, в чём состоит актуальность работы.

В главе 1 приводятся краткие теоретические сведения о криптографии.

В главе 2 приводятся краткие теоретические сведения из абстрактной алгебры.

В главе 3 представлены распространенные реализации ассиметричных криптоалгоритмов.

В главе 4 проанализированы известные атаки на системы «интернета вещей».

В главе 5 описана архитектура и способы проектирования систем «интернета вещей».

В главе 6 описан процесс разработки алгоритма аутентификации, а также приведены результаты тестирования малоресурсных криптографических алгоритмов.

В заключении приведены выводы о обеспечении информационной безопасности в системах «интернета вещей».

В приложении приложена программная реализация алгоритма RSA, а также криптографического алгоритма ГОСТ 28147-89.

ВЫВОДЫ

Объектом исследования данной работы являются особенности аутентификации в системах IoT. В ходе исследования выяснилось, что эти особенности главным образом проистекают из технических ограничений на размер устройства, его энергопотребление и цену. Так как эти устройства имеют разное предназначение и реализованы на разных платформах, реализация функций аутентификации, либо механизмов её составляющих, также будет различаться от платформы к платформе. Однако общие принципы аутентификации в системах IoT не отличаются от таковых в привычных информационных системах.

В результате проделанной работы можно сделать некоторые выводы о выборе и использовании алгоритмов шифрования для устройств ограниченной производительности. В зависимости от задачи можно обратиться к классическим либо к малоресурсным алгоритмам. Тесты показали, что стандарт ГОСТ 28147-89 прекрасно подходит для обеспечения безопасности в системах IoT. Однако, для устройств, реализованных на микроконтроллерах, его мощь может оказаться избыточной. В таком случае можно использовать специальные малоресурсные алгоритмы, и освободить драгоценные вычислительные и энергетические ресурсы для реализации полезных функции или обеспечения большей автономности. SPEC(64, 96) и TWINE-80 показали отличные результаты в тестах и могут использоваться в этом случае. Для реализации безопасного обмена ключами лучше по возможности пользоваться алгоритмами на эллиптических кривых, так как их реализации наиболее компактны и не уступают конкурентам по стойкости.

В силу специфики Интернета вещей, большую роль в обеспечении безопасности таких систем играют грамотно определенные политики безопасности. Зачастую именно разработчик аппаратного решения должен задумываться об этом, потому как от способа реализаций тех или иных механизмов обеспечения безопасности меняется способ взаимодействия устройств. Именно разработчик решает, например, как часто будут меняться ключи и каким образом они будут передаваться.

Исходя из анализа нескольких известных атак на системы IoT, можно предложить несколько решений которые инженер может применить для увеличения надежности своего устройства. Первое из таких решений – переход на аутентификацию по ключу, без использования паролей. Второе – регулярная смена ключей. Третье – передача ключей по внеполосным каналам. Всё это значительно усложнит задачу злоумышленника.

Как можно заметить из вышесказанного, основную роль в отражении атак на систему играет именно инфраструктурная безопасность. Грамотно спроектированная сетевая инфраструктура, тщательное тестирование системы на проникновение, и внимательно проработанные политики безопасности – залог надежности системы.

СПИСОК СОБСТВЕННЫХ ПУБЛИКАЦИЙ

[1-А.] Руденко Н.С. Особенности аутентификации в системах IoT / Н.С. Руденко, Г.А. Власова //54-ая научно-технической конференция аспирантов, магистрантов и студентов БГУИР – Минск, 2018.

[2-А.] Руденко Н.С. Особенности применения криптографических алгоритмов для аутентификации в системах IoT / Н.С. Руденко, Г.А. Власова // 16-ая Белорусско-российская научно-техническая конференция «Технические средства защиты информации» – Минск, 2018.