Сергиенко Е.Н., Савченко Е.С., Кальгов И.В., Редькина М.А. Интернет вещей в системах контроля и управления доступом. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVII Междунар. научно-техн. конф. – Пенза: ПДЗ, 2017. – С. 206-211.

УДК 004.056.53

ИНТЕРНЕТ ВЕЩЕЙ В СИСТЕМАХ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Е.Н. Сергиенко, Е.С. Савченко, И.В. Кальгов, М.А. Редькина

INTERNET OF THINGS IN PHYSICAL ACCESS CONTROL SYSTEM

E.N. Sergienko, E.S. Savchenko, I.V. Calgov, M.A. Redkina

Аннотация. Описывается понятие «Интернет вещей». Рассматривается технология бесконтактного взаимодействия RFID – радиочастотная идентификация. Определяются преимущества использования технологии RFID. Приводится понятие системы контроля и управления доступом. Представлен и описан перечень возможных сфер применения технологии RFID на основе алгоритмов низкоресурсной криптографии для СКУД. Обозначены некоторые алгоритмы малоресурсного шифрования, такие как TEA, DESL, а также семейство алгоритмов KATAN и KTANTAN.

Ключевые слова: информационная безопасность, Интернет вещей, RFID-технология, система контроля и управления доступом, низкоресурсная криптография, блочные шифры.

Abstract. The concept of the Internet of things is described. The technology of non-contact interaction RFID - radio frequency identification is considered. The advantages of using RFID technology are determined. The notion of an access control system is presented. A list of possible applications of RFID technology based on low-resource cryptography algorithms for ACS is presented and described. Some algorithms for low-resource encryption, such as TEA, DESL, as well as a family of algorithms KATAN and KTANTAN, have been designated.

Keywords: information security, Internet of Things, RFID-technology, physical access control system, low-level cryptography, block ciphers.

Технологии в наше время позволяют подключаться к сети Интернет многим вещам так, что из широкого арсенала датчиков, бытовых приборов и других предметов, имеющих активное подключение к сети, можно собрать сложную систему, выполняющую команды устройства управления, роль которых может выполнять любой гаджет. Это явление называется Интернетом вещей (InternetofThings, IoT) [1].

IoT уже пришел в повседневную жизнь через RFID (Radio Frequency Identification – радиочастотная идентификация) теги, штрих-коды на различных товарах. Радиочастотная идентификация – это современная технология, основанная на передаче с помощью радиоволн информации, необходимой для распознавания объектов, на которых закреплены специальные метки, несущие как идентификационную, так и пользовательскую информацию.

Во многих странах уже существуют в повседневном использовании такие устройства на основе RFID, как:

- микросхемы на таблетке, которые передают данные из желудка;

- датчики влажности, которые отправят вам SMS-сообщение, если затопило подвал, дом, квартиру;

- холодильник, который сам может заказать необходимые продукты в супермаркете.

Технология RFID широко используется в системах контроля и управления доступом для целей идентификации объектов доступа – людей или транспорта. Система контроля и управления доступом (СКУД) – это совокупность программных и технических средств, а также организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещением охраняемого объекта [2]. Такая система является элементом комплекса по обеспечению безопасности, рассматриваемого в статье [3].

Каждому посетителю предприятия, на котором внедрена СКУД, выдается идентификатор, несущий в себе RFID-метку. Такая RDIF-карта содержит уникальный идентификационный код и информацию о правах доступа. На основе сопоставления этой информации и уровня доступа помещения, куда попытается пройти предъявитель идентификатора, СКУД производит одно из действий: открывает дверь (замок, турникет, шлагбаум), блокирует доступ, ставит объект под охрану и т.д. На входе на территорию предприятия или в подлежащее контролю помещение установлен считыватель, который получает информацию с идентификатора и передает ее в централизованную систему контроля доступа. В статье [4] рассматриваются аспекты размещения и организации описанных выше технических устройств.

Использование технологии RFID приобрело большую популярность благодаря ряду преимуществ относительно других технологий, использующихся в идентификаторах для СКУД [5]:

- бесконтактная работа – RFID-метка может быть прочитана без какого-либо физического контакта между меткой и считывателем,
- работа вне прямой видимости,
- разнообразие диапазонов чтения,
- широкие возможности хранения данных – RFID-метка может хранить информацию до 10 000 байт на микросхеме площадью в $1см^2$,
- прочность – RFID-метки могут противостоять жестким условиям окружающей среды и имеют неограниченный срок эксплуатации,
- выполнение интеллектуальных задач – кроме хранения и передачи данных, RFID-метка может предназначаться для выполнения других задач.

Устройства IoT часто подвержены риску раскрытия или хищения конфиденциальной информации, хранящейся и передающейся при их взаимодействии. Для того чтобы противостоять таким угрозам, следует использовать криптографические алгоритмы шифрования - низкоресурсная криптография [6].

Взаимодействие между считывателем и идентификатором должно производиться в зашифрованном виде. RFID-метка позволяет хранить низкоресурсный алгоритм шифрования, используемый для обработки входных и выходных потоков данных. Это необходимо для того, чтобы информация, хранящаяся на метке, могла быть прочитана только владельцем считывателя с общим секретным ключом. Так как RFID-метки могут выполнять вычисление математических операций, необходимо записать на метку низкоресурсный алгоритм, который будет зашифровывать считываемые данные.

Целевым направлением развития низкоресурсной криптографии является применение и создание симметричных шифров, обладающих более высокой по

сравнению с асимметричными шифрами скоростью работы, что является критичным в рассматриваемых устройствах.

Рассмотрим некоторые основные алгоритмы низкоресурсного шифрования.

TEA – блочный алгоритм шифрования, основанный на сети Фейстеля. Шифр широко используется благодаря крайне низким требованиям к памяти и простоте реализации. Он имеет программную реализацию на разных языках программирования и аппаратную реализацию на интегральных схемах FPGA.

Алгоритм шифрования TEA основан на битовых операциях с 64-битным блоком, имеет 128-битный ключ шифрования. Стандартное количество раундов сети Фейстеля равно 64 (32 цикла), однако для достижения наилучшей производительности или шифрования число циклов можно варьировать от 8 (16 раундов) до 64 (128 раундов). Сеть Фейстеля несимметрична из-за использования в качестве операции наложения сложения по модулю 2^{32}.

Достоинствами шифра являются его простота в реализации, небольшой размер кода и довольно высокая скорость выполнения, а также возможность оптимизации выполнения на стандартных 32-битных процессорах, так как в качестве основных операций используются операции исключающего «ИЛИ», побитового сдвига и сложения по модулю 2^{32}. Поскольку алгоритм не использует таблиц подстановки и раундовая функция довольно проста, алгоритму требуется не менее 16 циклов (32 раундов) для достижения эффективной диффузии, хотя полная диффузия достигается уже за 6 циклов (12 раундов).

Алгоритм имеет отличную устойчивость к линейному криптоанализу и довольно хорошую к дифференциальному криптоанализу. Главным недостатком является его уязвимость к атакам «на связанных ключах» (англ. Related-keyattack). Из-за простого расписания ключей каждый ключ имеет 3 эквивалентных ключа. Это означает, что эффективная длина ключа составляет всего 126 бит, поэтому данный алгоритм не следует использовать в качестве хэш-функции.

Недостатком алгоритма является некоторая медлительность, вызванная необходимостью повторять цикл Фейстеля 32 раза, – это необходимо для тщательного «перемешивания данных» из-за отсутствия табличных подстановок.

Также стоит отметить, DESL – низкоресурсный алгоритм шифрования, нетребовательный к ресурсам, но достаточно криптостойкий. Он разработан на основе алгоритма DES. Для оптимизации использования DES в низкоресурсных условиях была проведена его модификация: были исключены перестановки IP и IP^{-1}, восемь оригинальных S-блоков были заменены одним, повторенным восемь раз. Авторами доказано, что данные изменения не влияют на стойкость алгоритма к линейному и разностным криптоанализам.

Недостатком данного шифра является малый размер ключа - 56 бит. Хотя для его раскрытия полным перебором требуются месяцы работы кластера из нескольких десятков компьютеров, на суперкомпьютере данная задача решается всего за три дня. Следовательно, подобный алгоритм стоит применять только там, где требуется краткосрочная защита или где важность защищаемых данных относительно невелика. Для реализации алгоритма необходимо 1848GE, что является приемлемым требованием для низкоресурсного шифра.

Также среди шифров низкоресурсной криптографии можно выделить семейства алгоритмов KATAN и KTANTAN. Каждое из семейств состоит из трех шифров, отличающихся размером блока шифрования: 32, 48 или 64. Все шифры имеют

80-битный ключ. Отличие KTANTAN от KATAN состоит в том, что первые требуют меньшее количество ресурсов благодаря тому, что ключ шифрования «вшит» в устройство и не может быть изменен. В описании шифров разработчиками показана стойкость к таким атакам, как разностный и линейный анализы, атака на связанных ключах и алгебраическая атака [7].

Библиографический список

1. Интернет вещей и всеобщий интернет [Электронный ресурс]. URL: http://www.bizhit.ru/index/trend_www_trafic/0-171

2. Контроль и управление доступом [Электронный ресурс]. URL: http://bolid.ru/projects/iso-orion/access-control/

3. Прокопенко А.Н., Ковалева Е.Г., Васюткина Д.И. Система оперативного управления комплексной безопасностью на основе информационных систем // Вестник БГТУ им. В.Г.Шухова. 2016. №2. С. 138-140.

4. Федотов Е.А., Федотова В.Н., Поляничка М.И. Некоторые аспекты модернизации ИТ-инфраструктуры предприятия. VII Международный молодежный форум “Образование. Наука. Производство”. Белгород, 2015.

5. Преимущества и недостатки внедрения RFID [Электронный ресурс]. URL:https://goo.gl/6QAzmv

6. Авезова Я. Новости криптографии: новые задачи и новые методы передовых направлений // CONNECT. 2014. №5. С. 72-75.

7. LW-криптография: шифры для RFID-систем. [Электронный ресурс]. URL:https://habrahabr.ru/post/119700

Сергиенко Елена Николаевна
Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия
E-mail: selena07@inbox.ru

Sergienko E.N.
Belgorod State Technological University named after V.G. Shukhov, Belgorod, Russia

Савченко Екатерина Сергеевна
Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия

Savchenko E.S.
Belgorod State Technological University named after V.G. Shukhov, Belgorod, Russia

Кальгов Илья Владимирович
Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия

Calgov I.V.
Belgorod State Technological University named after V.G. Shukhov, Belgorod, Russia

Редькина Маргарита Александровна
Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия

Redkina M.A.
Belgorod State Technological University named after V.G. Shukhov, Belgorod, Russia