www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2019.1.6

УДК 004.056.5
ББК 32.973

РАЗРАБОТКА БЕЗОПАСНОГО ПРОТОКОЛА СМАРТ ТЕХНОЛОГИЙ НА ОСНОВЕ СХЕМЫ ОДНОРАЗОВЫХ БЛОКНОТОВ С ПРИМЕНЕНИЕМ СИСТЕМ БЛИЖНЕГО ПОЛЯ ДЕЙСТВИЯ

Ирина Петровна Шумейко

Кандидат физико-математических наук, доцент,
заведующий кафедрой информационных систем,
Севастопольский государственный университет
IPShumejko@sevsu.ru, shumeyko-irina-74@yandex.ru
ул. Курчатова 7, 299015 г. Севастополь, Российская Федерация

Андрей Михайлович Пасечник

Магистрант кафедры информационной безопасности,
Севастопольский государственный университет
undeaddobbi@yandex.ru
ул. Курчатова 7, 299015 г. Севастополь, Российская Федерация

Аннотация. Целью данной статьи является разработка безопасного протокола для удаленного управления технологией «умный дом». В ходе исследования был разработан способ управления устройствами «интернета вещей» при помощи канала передачи информации в виде системы мгновенного обмена сообщениями в сети Интернет. Результатом данной работы является разработанный механизм для безопасного обмена данными между клиентом и сервером «умного дома».

Ключевые слова: информационная безопасность, защита данных, «интернет вещей», комплекс безопасности, «умный дом», мессенджеры, криптография, удаленный доступ, протоколы безопасной передачи данных.

Для взаимодействия с современной техникой при помощи сети интернет, предусмотрено большое количество механизмов удаленного управления. Все они так или иначе работают с пакетной передачей информации, но отличаются друг от друга алгоритмами формирования пакетов, их передачей, а также методам шифрования. Средства удаленного доступа представляют собой механизмы для связи как на локальном уровне, так и на глобальном (в сети интернет) [2; 4; 5].

Для организации работы сети «интернета вещей» требуется понимание работы портов сетевого оборудования и изучение механизмов их работы. Необходимо отметить, что существует несколько основных протоколов удаленного управления доступом, наиболее популярным из них является SSH. Терминальный доступ – является основным методом удаленного взаимодействия сетевых устройств, чаще всего, его работа организовывается при помощи протокола SSH (22 порт).

Особенностью данного протокола является – криптографическое преобразование всего потока данных при использовании данного протокола. Терминальный доступ – является основным методом удаленного взаимодействия сетевых устройств, чаще всего его работа организовывается при помощи протокола SSH (22 порт). Специалисты по аудиту безопасности пришли к выводу, что терминальный доступ наиболее безопасен, в сравнении с графическим. Использование удаленного узла можно отнести к эффективным способам обеспечения удаленного доступа сети «интернет вещей» [1]. Особенностью использования удаленного узла является возможность администратора войти в локальную сеть с такими же правами доступа, как и локальные пользователи данной сети. Виртуальные частные сети являются достаточно оптимальным способом безопасного подключения клиента к серверу. При использовании VPN производится аутентификация (подтверждение подлинности клиента), что повышает сетевую безопасность подключения. Протокол *https* является приемником протокола *http*, но с упором на безопасность данных и конфиденциальность клиентов при взаимодействии с сервером [6].

Наиболее эффективным, в плане безопасности канала передачи данных, является система мгновенных сообщений. Данный канал позволяет выполнять многие функции на порядок быстрее, также в его составе имеется специальный API для разработчиков «ботов», что позволяет расширить функционал и создавать нужные механизмы. Использование данного канала передачи данных помогает решить ряд проблем, связанных с авторизацией, аутентификацией и идентификацией пользователей системы [3].

Наиболее подходящим вариантом для реализации является одноплатный компьютер Raspberry Pi model B. Характерным минусом является скорость отклика на команды ввиду многозадачности процессора, но данный факт не является критичным при поставленной задаче. Положительным аспектом выбора является полноценная система, на базе которой возможно запустить веб-сервер, хостинг сайта состояния устройств «умного дома», а также возможность использования основных языков программирования для реализации проекта. Одноплатный компьютер позволяет производить действия с большей скоростью и комфортом для пользователя, не требует глубоких знаний программирования для создания и реализации задач, позволяет более эффективно автоматизировать процессы управления.

Веб-сервера делятся на две категории: те, что поддерживают динамический и статический контент и те, что поддерживают только статический. Данный фактор является ключевым при выборе сервера под определенные задачи системы.

Наиболее целесообразно использовать операционную систему семейства Linux по большому ряду причин.

Выбор стека технологий влияет на общую концепцию системы и вносит свои коррективы. Оптимальный выбор всех программных и программно-аппаратных элементов задает вектор работы всей системы и позволяет создать более эффективную систему в целом. Использование веб-приложения облегчает пользователю возможность взаимодействия с устройствами «умного дома», а технология AJAX позволяет автоматизировать процесс фонового обмена данными с сервером. Шифр Вернама дает возможность сделать соединение абсолютно криптостойким, а способность взаимодействия по двум каналам связи делает данный протокол более универсальным для разных групп пользователей.

Для реализации работы протокола безопасного обмена данными был разработан стек механизмов, которые в совместном использовании генерируют безопасный протокол. Для общей защиты всей системы используется два механизма. При работе клиента и веб-приложения создается безопасное *https* соединение, которое шифрует передаваемые данные между браузером пользователя и сервером сайта. Данный параметр позволяет решить ряд задач, связанных с информационной безопасностью Интернет-соединения.

При использовании веб-приложения – необходимо пройти авторизацию, чтобы попасть на страничку централизованного управления и мониторинга электроприборов «умного

дома». Само *https* соединение необходимо для того, чтобы исключить компрометацию передаваемых данных пользователем или сервером, потому как состояние устройств дома хранится в файле, который взаимодействует с сайтом.

Для работы с ботом необходимо пройти этап синхронизации смартфона и модуля NFC. На сервере генерируется одноразовый блокнот заданной длины. Пользователь подносит свой телефон к модулю и считывает с него данные, иными словами, проходит синхронизацию, на устройстве появляется одноразовый блокнот, точно такой же, как и на сервере. А для работы с данным криптографическим алгоритмом, клиент и сервер должны договориться о длине ключа, так как ключ должен быть равен длине передаваемого сообщения. Далее ключ используется на следующем этапе взаимодействия.

Следующим пунктом работы протокола является управление пользователя системой через бот, при использовании данного канала передачи данных реализовано дополнительное шифрование в виде одноразового блокнота. Само соединение внутри канала передачи шифруется алгоритмом, поддерживаемым системой (как правило, это Signal или MTProto), но для большей безопасности используется алгоритм Вернама. В данном протоколе пользователь вручную шифрует данные своим блокнотом и отправляет это сообщение боту, который в свою очередь производит расшифровку и выполнение команд. После отправки каждой команды из блокнотов вычеркивается использованная часть. Размер блокнота должен быть выбран таким образом, чтобы пользователь имел запас для работы хотя бы на несколько дней.

Протокол позволяет управлять домом при помощи сайта и при помощи «бота», а наиболее безопасным способом является взаимодействие через систему мгновенных сообщений. На рисунке представлена общая схема работы всего алгоритма безопасного обмена данными.

Данный протокол является уникальным решением для защиты каналов обмена информации в сфере устройств «интернета вещей», а также в целом всей концепции «умного дома». Реализация поставленных задач полностью достигнута, а данный протокол может быть использован в реальных условиях. Актуальность защиты информации в «умных домах» является основополагающим моментом при развитии данной технологии. Разработка данного протокола позволяет вывести информационную безопасность домов на новый уровень. Проект может быть использован в массовом потреблении, а сам безопасный механизм стать неотъемлемой частью в домах будущего.

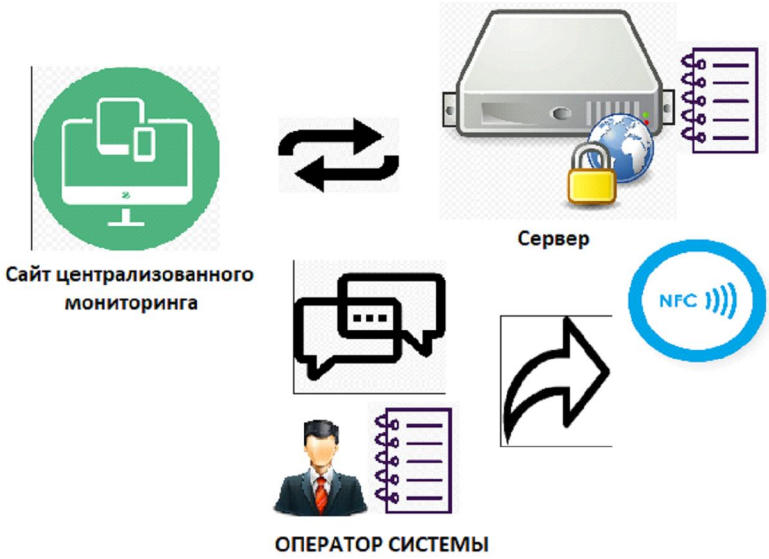

Рисунок. Протокол безопасного взаимодействия смарт технологий

СПИСОК ЛИТЕРАТУРЫ

1. Баричев, С. Г. Основы современной криптографии / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. – Москва : СИНТЕГ, 2011. – 176 с.

2. Гатченко, Н. А. Криптографическая защита информации / Н. А. Гатченко, А. С. Исаев, А. Д. Яковлев ; под общ. ред. Н. А. Гатченко – СПб. : НИУ ИТМО, 2012. – 142 с.

3. Голобродский, К. Б. Знакомьтесь: Ubuntu. – Ростов н/Д. : Феникс, 2010. – 160 с.

4. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / под ред. проф. В. Г. Кузьмина. – 5-е изд. – СПб. : Питер, 2016. – 992 с. : ил.

5. Основы локальных компьютерных сетей : учебник / под ред. проф. М. С. Петрова – СПб. : Издательство «Лань», 2016. – 184 с. : ил. – (Учебники для вузов. Специальная литература).

6. Программирование на Python : учебник / под ред. М. А. Синявина. – СПб. : Символ-Плюс, 2011. – 992 с., ил.

REFERENCES

1. Barichev S.G., Goncharov V.V., Serov R.E. *Osnovy sovremennoy kriptografii* [Basics of Modern Cryptography]. Moscow, SINTEG Publ., 2011. 176 p.

2. Gatchenko N.A., Isaev A.S., Yakovlev A.D. *Kriptograficheskaya zashchita informatsii* [Cryptographic Protection of Information]. Saint Petersburg, NIU ITMO Publ., 2012. 142 p.

3. Golobrodskiy K.B. *Znakomtes: Ubuntu* [Meet Ubuntu]. Rostov-on-Don, Feniks Publ., 2010. 160 p.

4. Kuzmin V.G., ed. *Kompyuternye seti. Printsipy, tekhnologii, protokoly: uchebnik dlya vuzov* [Computer Network. Principles, Technologies, Protocols: Textbook for Universities]. Saint Petersburg, Piter Publ., 2016. 992 p.

5. Petrov M.S., ed. *Osnovy lokalnykh kompyuternykh setey: uchebnik* [Fundamentals of Computer Networks. Textbook]. Saint Petersburg, Izdatelstvo «Lan», 2016. 184 p.

6. Sinyavin M.A., ed. *Programmirovanie na Python: uchebnik* [Programming in Python. Textbook]. Saint Petersburg, Simvol-Plyus Publ., 2011. 992 p.

THE DEVELOPMENT OF SECURE PROTOCOL IN SMART TECHNOLOGIES FOR SCHEMA-BASED ONE-TIME PADS USING THE SYSTEM OF NEAR-FIELD ACTIONS

Irina P. Shumeiko

Candidate of Sciences (Physics and Mathematics),
Head of the Department of Information Systems,
Sevastopol State University
IPShumejko@sevsu.ru, shumeyko-irina-74@yandex.ru
Kurchatova St., 7, 299015 Sevastopol, Russian Federation

Andrey M. Pasechnik

Master Student, Department of Information Security,
Sevastopol State University
undeaddobbi@yandex.ru
Kurchatova St., 7, 299015 Sevastopol, Russian Federation

Abstract. Interacting with modern technology using the Internet provides a large number of remote control mechanisms. All of them somehow work with packet data transmission, but differ from each other by algorithms of packet formation, their transmission, as well as encryption methods. Remote access tools are mechanisms for communication both locally and globally (on the Internet). The purpose of this article is to develop a secure Protocol for "smart home" remote control technology. In the course of the study, a method was developed to control the devices of the "Internet of things" using the channel of information transmission in the form of instant messaging system on the Internet. The result of this work is a developed

mechanism for secure data exchange between the client and the "smart home" server. This Protocol is a unique solution for protecting information exchange channels in the field of "Internet of things" devices, as well as the whole concept of "smart home". The implementation of the tasks is fully achieved, and this Protocol can be used in real conditions. The relevance of protecting information in "smart homes" is a fundamental point in developing this technology. Developing this Protocol allows you to bring the information security of homes to a new level. The project can be used in mass use, and the safe mechanism can become an integral part in the homes of the future.

Key words: information security, data protection, "Internet of things", security complex, "smart home", messengers, cryptography, remote access, secure data transfer protocols.