УДК 004.056.55

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕТОДОВ АУТЕНТИФИКАЦИИ И УПРАВЛЕНИЯ ДОСТУПОМ К ИНФОРМАЦИОННЫМ СИСТЕМАМ

© 2024 Л. С. Крыжевич[1], М. С. Кофанов[2]

[1]кандидат технических наук, и.о. завкафедрой информационной безопасности
e-mail: leonid@programist.ru
[2]бакалавр направления подготовки «Информационная безопасность»
e-mail: mat55502@gmail.com

Курский государственный университет

В статье проводится анализ существующих систем аутентификации и управления доступом, их видов, особенностей работы и эксплуатации, а также представлена авторская разработка такой системы.

Ключевые слова: аутентификация, безопасность, управление доступом, микроконтроллер, WiFi-модуль, плата, информация интерфейс.

RESEARCH AND DEVELOPMENT OF AUTHENTICATION AND ACCESS CONTROL METHODS FOR INFORMATION SYSTEMS

© 2024 L. S. Kryzhevich[1], M. S. Kofanov[2]

[1]Candidate of Technical Sciences
e-mail: leonid@programist.ru
[2] Bachelor, Department of Information Security
e-mail: mat55502@gmail.com

Kursk State University

This research paper analyzes existing authentication and access control systems, their types, operating characteristics, and implementation, and presents the author's own development of such a system.

Keywords: Authentication, Security, Access Control, Microcontroller, WiFi Module, Board, Information Interface.

За последние десятилетия информационные технологии прочно вошли в нашу жизнь, став незаменимым инструментом во всех сферах деятельности. Передовые разработки и современные информационные системы позволяют эффективно управлять данными, решать сложные задачи и обеспечивать бесперебойную работу организаций. Желание людей сделать свою жизнь более комфортной, удобной и технологичной подтолкнуло сферу Интернета вещей (IoT) к стремительному росту и развитию все более новых разработок, инноваций и технических решений. Одним из интересных примеров внедрения технологий IoT стали умные сейфы. Это не просто прочные хранилища, а полноценные «умные» системы с современными техническими решениями в области защиты содержимого и управления доступом. Данные «умные» сейфы могут различные методы аутентификации, оснащены удаленным управлением и обладают интеграцией с системами «умного дома» [1].

Однако с появлением все более сложных и развитых технологий возникают и новые угрозы безопасности информации. Устройства IoT недостаточно защитить на физическом уровне, необходимо также обеспечить защиту информационных систем, их целостность, доступ и бесперебойную работу. В 2023 г. и начале 2024 г. ситуация с киберугрозами, направленными против устройств IoT, претерпела значительные изменения. Согласно статистике, в 2023 г. количество вредоносных программ для IoT увеличилось на 400% по сравнению с предыдущим годом. Этот рост в значительной степени обусловлен тем, что киберпреступники используют критические уязвимости в устройствах IoT.

Методы аутентификации и управление доступом являются одними из основных мер в обеспечении безопасности информационных систем. С развитием цифровых технологий и увеличением количества подключенных устройств требования к безопасности также значительно возрастают [2].

Актуальность данной темы основывается на повышении значимости безопасности информационных систем. Верные методы аутентификации и эффективное управление доступом позволяют минимизировать риски несанкционированного доступа и утечки информации.

Теоретические основы и принципы работы устройств управления доступом

В современном информационном обществе безопасность информации является одним из важнейших аспектов функционирования организаций и отдельных пользователей.

Обеспечение безопасности сферы Интернета вещей приобретает все большее значение по мере расширения использования этих устройств в повседневной жизни и промышленности. Устройства IoT обеспечивают удобство и автоматизацию, но одновременно создают новые уязвимости для кибератак. Согласно отчету Symantec, в 2023 г. количество атак на IoT-устройства достигло более 1,5 млрд попыток взлома. Чаще всего в атаках задействуются устройства с минимальной защитой, такие как камеры видеонаблюдения, маршрутизаторы и умные бытовые приборы. Эти устройства становятся мишенями для DDoS-атак и несанкционированного доступа из-за слабых паролей, неправильных настроек политик безопасности и редких обновлений программного обеспечения.

Перечислим основные уязвимости устройств Интернета вещей (IoT).

1. Слабые методы аутентификации и пароли. Многие IoT-устройства поставляются с предустановленными паролями, которые пользователи часто не меняют или используют слабые пароли, что делает устройства легкой мишенью для злоумышленников.

2. Недостаточная защита данных. Отсутствие шифрования при передаче данных и хранении на устройствах может привести к утечкам конфиденциальной информации.

3. Ограниченные возможности мониторинга и управления. Многие IoT-устройства не имеют встроенных механизмов для обнаружения и предотвращения вторжений.

4. Недостаточная сегментация сети. Устройства часто подключаются к той же сети, что и критически важные системы, что позволяет злоумышленникам проникнуть в сеть через менее защищенные устройства.

5. Физический доступ к устройствам. Многочисленные IoT-устройства размещаются в легкодоступных местах и не имеют какой-либо надежной физической защиты. Корпус обычно сделан из не особо прочных, компонентов, и его легко вскрыть, чтобы получить доступ к блоку управления устройства [3].

Одной из основных задач в области защиты информации является аутентификация пользователей и управление доступом к информационным ресурсам.

Аутентификация – это процесс проверки подлинности обращения, предъявляемого субъектом системы, а также проверки соответствия субъекта предъявляемым системой данным. Управление доступом же определяет права и привилегии каждого пользователя в системе и контролирует его действия при взаимодействии с информационными ресурсами [4].

Существует несколько основных методов аутентификации и управления доступом к информационным системам. Один из наиболее распространенных методов – это парольная аутентификация. Пользователь предоставляет системе установленный им пароль, который затем сравнивается с предопределенным значением. Пароль может быть одноразовым, статическим или динамическим, а также может быть усилен различными технологическими средствами, такими как хеширование или шифрование [5].

Другим методом аутентификации является использование биометрических данных, таких как отпечатки пальцев, радужная оболочка глаза, голосовые данные и другие. Эти данные сравниваются с заранее сохраненными шаблонами в базе данных системы, и в случае совпадения пользователю предоставляется доступ [6].

Также существуют методы аутентификации на основе аппаратных средств, например, использование смарт-карт или USB-токенов. Пользователь предъявляет системе физическое устройство, содержащее его уникальный идентификатор или сертификат, который используется для проверки доступа [7].

Разработка устройства аутентификации и управления доступом

В рамках задачи по созданию собственного устройства аутентификации и управления доступом был разработан программно-аппаратный комплекс аутентификации на базе микроконтроллера Arduino Uno. Устройство представляет собой сейф, дополненный информационной системой с облачным хранилищем данных о пользователях данного сейфа, а также содержащихся вещах и системой управления доступом на базе микроконтроллера [8].

Общая концепция заключается в следующем: доступ к сейфу возможен либо при вводе пароля, либо при предъявлении доверенного ключа(RFID-токена), при этом все действия с данными методами аутентификации регистрируются в журнале событий. Кроме того, при получении доступа к самому сейфу пользователь работает непосредственно с информационной системой, которая реализует функцию «инвентаризации» при добавлении или удалении вещей из физического хранилища. Функция «инвентаризации» заключается в том, что предмет, который пользователь хочет положить в физическое хранилище, можно также добавить в информационную систему. Такой предмет должен быть оснащен собственным RFID-токеном. Таким образом, при выборе определенных настроек работы комплекса пользователь может добавить предмет в информационную систему, где он и будет числиться. Информацию о данном предмете можно увидеть как в самом программно-аппаратном комплексе, так и на разработанном веб-сайте. Тем самым результат действий пользователь тоже передается в зашифрованном виде и представляется в виде текущего состояния «хранилища» содержимого сейфа в базе данных. Доступ к БД происходит через веб-сайт. Данную систему можно условно разделить на несколько блоков.

Первый блок включает в себя само физическое хранилище, сейф. Блок состоит из замка дверок, RFID модуля считывания, приспособления парольного ввода, блока управления. Блок управления – это ключевой элемент данной системы, в этом устройстве происходят все основные действия и алгоритмы по аутентификации пользователей, записи результатов предыдущего процесса и шифрованию результата работы этой системы. Связь элементов системы представляется следующим образом: замок двери, RFID модуля считывания и устройство парольного ввода связаны с

блоком управления посредством соединительных проводов, при подносе ключа доступа (RFID-метки) происходит алгоритм проверки данного токена с доверенными ключами, предварительно добавленными в систему, результат шифруется, передается в следующий блок с помощью канала связи в сеть Интернет в базу данных. То же самое происходит в случае предоставления системе пароля на вход, результат работы алгоритма шифруется и передается через канал связи в базу данных. При успешной аутентификации пользователь получает доступ к информационной системе комплекса. Результаты работы пользователя с системой также обрабатываются, шифруются и отсылаются с помощью канала связи в сеть Интернет.

Второй блок включает в себя облачное хранилище, состоящее из базы данных, WEB-сайта со встроенной функцией расшифровки данных. В облачное хранилище по каналу связи поступает зашифрованная информация, которая записывается в базу данных. Для отображения содержимого базы данных используется разработанный веб-сайт. Для расшифровки и просмотра информации в первоначальном виде используются отдельные функции сайта.

Для инициализации системы нужен RFID-токен, который прикладывается к модулю считывания и передает сигнал о том, что предоставлен ключ доступа и необходимо запустить алгоритм аутентификации. Следующее действие – сравнение предоставленного ключа с предустановленными доверенными ключами в системе. В микроконтроллер приходит статус сравнения. Если статус является положительным, то посылается сигнал на релейный модуль, который, в свою очередь, отпирает электрозамок. В противном случае предыдущие действия пропускаются. Подобный порядок происходит и при парольном методе доступа. Введенный пользователем пароль сравнивается с установленным системным паролем, и в случае соответствия подается сигнал на релейный модуль. Важно отметить, что разрабатываемый программно-аппаратный комплекс выполнен с двумя отдельными ячейками для хранения. В данном случае реализовано управление доступом по двум ячейкам. Оба хранилища запираются на электрозамки, однако имеют разные способы аутентификации: первая ячейка может быть открыта только с помощью доверенного ключа доступа, тогда как вторая имеет как парольный, так и доступ по RFID-ключу. Для каждой из ячеек используются разные ключи доступа для реализации функции управления и контроля доступа. Соответственно, от того, какая ячейка была открыта, зависит, с какой из них информационная система будет в текущий момент работать. В микроконтроллере происходит шифрование, и статус работы системы аутентификации отправляется с помощью подключения к сети Интернет посредством технологии Wi-Fi в зашифрованном виде в облачное хранилище, где записывается в базу данных. Для доступа в облачное хранилище имеется веб-страница, на которой отображается информация, взятая из базы данных и расшифрованная для удобной с ней работы.

В состав устройства аутентификации и управления доступом входят следующие компоненты:

- микроконтроллер Wemos D1 R1 с WiFi модулем ESP 8266 для доступа к беспроводной сети и отправки данных,
- LCD 1602 (I2C) – LCD-дисплей с I2C-интерфейсом для отображения данных,
- матричная мембранная клавиатура 4x4,
- RFID-модуль RC-522 с набором бесконтактных карт-ключей,
- 2 релейных модуля,
- пьезоэлектрический излучатель (буззер),
- MB-102 – макетная плата для сборки тестового образца,
- соединительные провода.

Весь проект реализуется на основе платы Arduino Uno R3 на базе процессора ATmega328P. Плата обладает шиной I2C, а также памятью в 2 кб SRAM, 32 кб FLASH, 1 кб EEPROM, которая необходима для сбора, хранения и обработки информации при работе устройства [9].

Кроме того, разработанное устройство оснащено доступом к беспроводной сети Wi-Fi посредством платы на базе микроконтроллера Wemos D1 R1 с Wi-Fi-модулем ESP8266. Таким образом, осуществлена функция «инвентаризации», а также, с учетом наличия двух релейных модулей, реализовано разделение доступа в виде двух отдельных ячеек сейфа [10].

Программно-аппаратный комплекс аутентификации и управления доступом «Умный сейф» можно рассмотреть как комбинирование методов аутентификации и управления доступом: парольного ввода и RFID-модуля считывания токенов, а также функционирование информационной системы с поддержкой разработанного веб-сайта. С помощью данных методов пользователь получает доступ к системе [11].

Таким образом, с учетом всех особенностей и условий использования систем аутентификации и управления доступом разработанный программно-аппаратный комплекс имеет следующие преимущества:

1) универсальность и доступность: Arduino Uno – это распространенная и популярная платформа, которая достаточно проста в использовании и доступна для множества разработчиков;

2) разнообразие методов аутентификации: разработанный комплекс включает в себя несколько методов аутентификации, таких как доступ по паролю и доступ по RFID-токенам. Это позволяет адаптировать систему под различные требования безопасности и предпочтения пользователей;

3) гибкость настройки и обновления: Arduino Uno имеет возможность программной настройки и обновления функционала.

Библиографический список

1. Arduino Uno R3 [Официальный сайт]. – URL: https://store.arduino.cc/arduino-uno-rev3 (дата обращения: 20.10.2023).

2. Как подключить RFID-модуль RC522 к Arduino [Электронный ресурс]. – URL: https://роботехника18.рф/rfid-rc522/ (дата обращения: 23.10.2023).

3. Работа с символьным ЖК дисплеем 1602 [Электронный ресурс]. – URL: https://wiki.iarduino.ru/page/Working_with_character_LCD_displays (дата обращения: 22.10.2023).

4. Arduino IDE [Официальный сайт]. – URL: https://www.arduino.cc/en/software (дата обращения: 15.09.2023).

5. *Крыжевич, Л. С.* Учебное пособие по микроконтроллеру Atmega 328. Ч. 1. – Курск: Курский электромеханический техникум, 2017. – 220 с.

6. *Крыжевич, Л. С.* Учебное пособие по микроконтроллеру Atmega 328. Ч. 2. – Курск: Курский электромеханический техникум, 2017. – 175 с.

7. *Крыжевич, Л. С.* Учебное пособие по микроконтроллеру Atmega 328. Ч. 3. – Курск: Курский электромеханический техникум, 2017. – 244 с.

8. *Семенов, Б. Ю.* Шина I2C в радиотехнических конструкциях. – Москва: СОЛОН-Р, 2002. – 190 с.

9. *Белов, А. В.* Программирование ARDUINO. Создаем практические устройства – Санкт-Петербург: Наука и техника, 2018. – 272 с.

10. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учебное пособие / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов, Э. Р. Газизова; под ред. А. А. Шелупанова. – Москва, 2012. – 550 с.

11. Программируем Arduino. Профессиональная работа со скетчами. – Санкт-Петербург: Питер, 2017.