ВЕСТНИК ЮГОРСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
2019 г. Выпуск 2 (53). С. 23–28

DOI: 10.17816/byusu20190223-28
УДК 681.5:621.38

Е. А. Годовников, А. В. Шицелов, Р. Т. Усманов

ПРОЕКТИРОВАНИЕ СКУД ПРЕДПРИЯТИЯ С ИНТЕГРИРОВАННОЙ АУТЕНТИФИКАЦИЕЙ БЕСПРОВОДНОЙ СЕТИ

В данной статье рассматривается проектирование системы контроля и управления доступом для предприятия с различными способами аутентификации и идентификации пользователей. Был проведен обзор существующих решений в области проектирования систем контроля и управления доступом. В ходе работы был предложен проект системы, а также были подробно описаны ее составные части.

Ключевые слова: СКУД, система контроля и управления доступом, автоматизированная система управления, NFC, iButton, идентификация, аутентификация, проектирование системы.

E. A. Godovnikov, A .V. Shitselov, R. T. Usmanov

DESIGN OF PHYSICAL ACCESS CONTROL SYSTEM WITH INTEGRATED WIRELESS AUTHENTICATION

This article discusses the design of a physical access control system for an enterprise with various methods of authentication and user identification. A review of existing solutions in the design of physical access control systems was conducted. In the course of the work, a system design was proposed, and its components were described in detail.

Keywords: PACS, physical access control system, automated control system, NFC, iButton, identification, authentication, system design.

I. Введение

Система контроля удаленного доступа (СКУД) с электромеханическими замками стала необходимой частью любого крупного учреждения. Чем больше помещений, тем больше ключей, которые приходится носить с собой или брать их на вахте, что также тратит дополнительное время сотрудников. Современным вариантом решения проблемы является открытие дверей при помощи электронного ключа или телефона [1, 2].

II. Проектирование

На сегодняшний день существуют различные способы аутентификации пользователя в системах СКУД:

- аутентификация по паре логин/пароль – самая простая аутентификация. Для ее реализации надо всего лишь проверить пару логин/пароль на наличие в базе данных пользователей. Недостатком данного метода является необходимость знать пару логин и пароль;
- аутентификация по технологии NFC (RFID) [3, 4, 5] – преимуществом данного способа аутентификации является то, что пользователю не надо вводить какие-либо данные, сам NFC-чип уже содержит всю необходимую информацию для аутентификации пользователя. Недостатком NFC будет являться необходимость наличия физического устройства (NFC-чипа) у пользователя;
- аутентификация по ключам iButton – обладает все теми же преимуществами и недостатками, что и NFC. Однако iButton обладает одним преимуществом перед NFC – это более простая и дешевая реализация как физического устройства, так и протокола передачи данных.

Функциональные требования

Согласно изложенным выше способам аутентификации и требованиям к системе [1], проектируемая система должна реализовывать следующие функции:

- авторизация пользователя через Wi-Fi-сеть;
- предоставление доступа к помещению через NFC-ключ;
- предоставление доступа к помещению через QR-код;
- регистрация событий открытия двери помещения с помощью обычного ключа;
- ведение журнала доступа пользователей в помещение.

Общая концепция системы

Согласно функциональным требованиям система должна уметь автоматически авторизовать пользователя в системе в тех случаях, когда он подключен к Wi-Fi-сети организации, а также поддерживать открытие двери по NFC-метке и QR-коду с ведением журнала доступа. Разберем каждую из частей отдельно.

Открытие двери по QR-коду

Начнем с наиболее простой задачи: открытие двери по QR-коду. Для ее решения предположим, что у нас есть некоторая система, которая умеет авторизовать пользователя по логину и паролю и предоставляет веб-интерфейс, в котором можно по нажатию кнопки открыть дверь. Тогда самым простым решением данной задачи будет сделать QR-коды со ссылкой на кнопку открытия двери. Тут сразу же стоит отметить, что в случае если пользователь не авторизован и не имеет прав, система должна перенаправить на страницу входа или же сообщить об отсутствии прав.

Авторизация посредством опознавания устройства в Wi-Fi-сети

Следующим шагом станет создание концепции автоматического входа пользователя в систему в том случае, если он зашел на форму входа из Wi-Fi-сети организации.

Так как в организации используется единая точка входа для всех клиентов Wi-Fi-сети и тип авторизации EAP, предлагается подключиться к шлюзу авторизации и при обнаружении нового пользователя в системе попытаться получить о нем информацию из шлюза авторизации Wi-Fi-сети [6].

Вход в помещение через NFC-метку, открытие двери и событие оповещения о доступе в помещение

Теперь стоит продумать способ открытия двери с сайта. Тут сразу же стоит отметить, что сайт является единой точкой управления всеми дверьми, к которому в небольшие интервалы времени будет обращаться большое количество людей, и система должна дать ответ каждому пользователю в приемлемое время. С другой стороны, необходимо управлять замком каждой двери в отдельности, а на открытие замка двери уходит некоторое время. Из этого следует, что нельзя управлять замком двери напрямую с сайта.

Для решения этой проблемы систему можно разделить на две части:

1. Веб-сайт, отвечающий за авторизацию, контроль доступа и инициирование команд управления дверьми.

2. Модуль управления замком двери, отвечающий за исполнение команды и обнаружение событий открытия двери.

Из этой архитектуры следует, что необходимо сделать интерфейс взаимодействия двух частей системы. Поскольку запросы к веб-сайту идут по протоколу HTTP, то лучше и проще всего реализовать взаимодействия между частями системы через REST.

Теперь стоит подумать об открытии двери NFC-картой. Поскольку устройство для считывания NFC-карты будет находиться рядом с дверью, то логичнее всего взаимодействовать с ним через модуль управления замком. Второй проблемой NFC будет аутентификация карты в системе – за эту часть отвечает веб-сайт. Из этого следует, что необходимо учесть возможность подтверждения карты через веб-сайт.

Протокол взаимодействия между системами

Для взаимодействия между системами будем использовать REST [7]. Теперь необходимо определиться с системой команд и форматом обмена данными, для этого определим, какими данными необходимо обмениваться двум частям системы (в данном случае сервер – это веб-сайт, а клиент – модуль управления замком):

- команда на открытие/закрытие замка (от сервера к клиенту);
- команда на подтверждение доступа по карте (от клиента к серверу);
- добавление удаления ключей;
- событие открытие/закрытие двери (от клиента к серверу);
- событие открытие/закрытие замка (от клиента к серверу).

Команда на открытие/закрытие замка

Данная команда предназначена для управления замком и может посылаться как от сервера к клиенту, так и от клиента к серверу. Однако значения данных команд будут немного разные:

- Если сервер посылает данную команду клиенту, то это прямая команда на открытие замка, и клиент должен ее исполнить.
- Если команду посылает клиент серверу, то это запрос на доступ к двери, при этом клиент должен указать дополнительные параметры в запросе, а именно ID ключа и тип ключа (NFC или iButton). В случае если сервер успешно выполнит запрос, то клиент должен открыть замок (дверь).

Данная команда может иметь следующие параметры:

- id –уникальный идентификатор замка;
- type – тип ключа (NFC или iButton), используется только если запрос посылает клиент;
- key – сам ключ.

Стоит обратить внимание, что в команде явно не указывается, что надо сделать с дверью (открыть или закрыть). Это сделано потому, что команда работает как инвертер, т. е. каждый ее вызов изменяет состояние замка на противоположный.

Формат запроса представлен на листинге 2.1.

Листинг 2.1 – Формат запроса на открытие замка в формате JSON

```
{
    "id": "1",
    "type": "NFC",
    "key": "123-123-321-abc-"
}
```

Добавление/удаление ключей

Данная команда нужна для регистрации и удаления ключей (NFC или iButton). Посылается от клиента к серверу и просто добавляет в базу один новый ключ или удаляет его.

Параметры:
- id – id в формате UUID;
- type – тип ключа;
- action – тип операции (добавить (add) или удалить (remove).

Формат запроса представлен на листинге 2.2.

Листинг 2.2 – Формат запроса на открытие замка в формате JSON

```
{
    "id": "123-321",
    "type": "ibutton",
    "action" : "remove"
}
```

Событие открытие/закрытие двери

Данный тип команд посылается только клиентом к серверу и служит для оповещения последнего о событиях, происходящих с дверью.

Имеет 2 параметра:
- id – идентификатор двери;
- status – что произошло с дверью (возможные состояния открыта (open) и закрыта (close).

Пример запроса представлен на листинге 2.3.

Листинг 2.3 – Команда оповещения сервера о состоянии двери в формате JSON

```
{
    "id": "123-321",
    "status": "close"
}
```

Событие открытие/закрытие замка

Данный тип команд посылается только клиентом к серверу и служит для оповещения последнего о событиях, происходящих с замком.

Имеет 4 параметра:
- id – идентификатор замка;
- status – что произошло с замком (возможные состояния открыта (open) и закрыта (close);
- key – id ключа (если событие было вызвано с использованием ключа);
- type – тип ключа (если событие было вызвано с использованием ключа).

Пример запроса представлен на листинге 2.4.

Листинг 2.4 – Команда оповещения сервера о состоянии замка в формате JSON

```
{
    "id": "123-321",
    "status": "open",
    "key": "123-123",
    "type": "NFC"
}
```

Проектирование базы данных

Для начала необходимо определить, какие данные мы будем хранить в системе:

1. Список дверей.
2. Состояние дверей (замков).
3. Пользователи и их права.
4. Журнал доступа.

На основе каждого из этих пунктов составим схему базы данных (рис.).

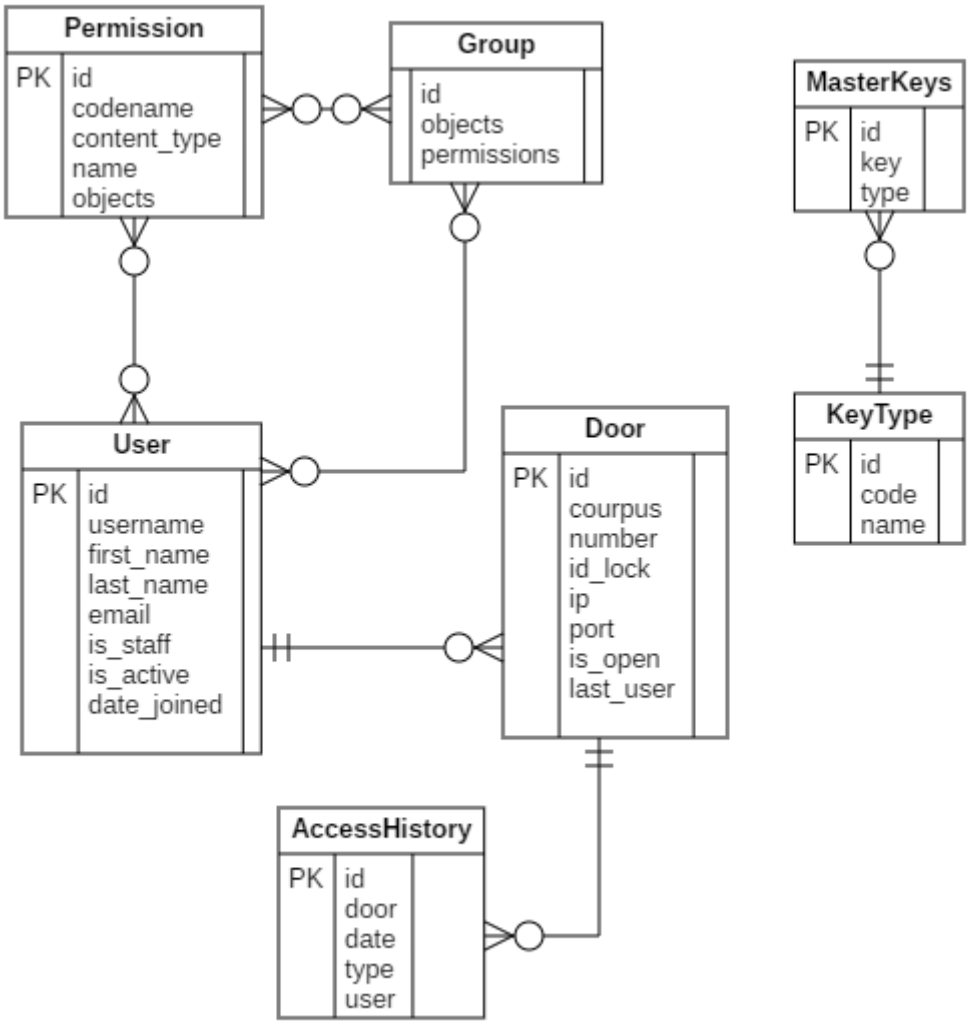

Рисунок – Схема базы данных

III. Заключение

В результате проделанной работы была спроектирована система контроля удаленного доступа (СКУД) с электромеханическими замками с возможностью доступа к системе посредством NFC-чипов, iButton-ключей, QR-кода, корпоративной беспроводной сети (Wi-Fi) или же простого входа по паре логин/пароль.

Предложенное решение было спроектировано с учетом возможности осуществлять вход пользователя в систему через разные способы аутентификации и предоставления ему выбора наиболее удобного для него способа войти в систему или открыть дверь.

Также был разработан протокол связи сервера системы с подчинёнными устройствами (замками), посредством которого и осуществляется непосредственное управление дверью

(замком) с возможностью двунаправленной связи клиента с сервером и системой событий состояния как двери, так и замка.

Литература

1. Годовников, Е. А. СКУД офисного помещения. Выбор архитектуры / Е. А. Годовников, Р. Т. Усманов, А. В. Шицелов. – Текст : непосредственный // Евразийское научное объединение. – 2018. – № 46. – С. 67–69.

2. Максимов, Р. Л. Разработка автоматической СКУД повышенной безопасности на базе типового решения СКУД BioSmart с использованием автоматного подхода / Р. Л. Максимов, А. Г. Рафиков. – Текст : непосредственный // Вопросы кибербезопасности. – 2015. – № 13. – С. 73–80.

3. Нуйкин, А. В. Использование RFID-технологии в экосистеме интернета вещей / А. В. Нуйкин, А. С. Кравцов. – Текст : непосредственный // Сборник тезисов 3-й Международной научной конференции «Международный форум «Микроэлектроника-2017». – Москва, 2017. – С. 279–281.

4. Исхаков, А. Ю. Схемы аутентификации пользователя в СКУД с использованием QR кодов и передачи данных по технологии NFC / А. Ю. Исхаков, Р. В. Мещеряков. – Текст : непосредственный // Информационное противодействие угрозам терроризма. – 2014. – № 22. – С. 11–15.

5. Рабинович, А. С. Аутентификация пользователя информационной системы с использованием технологии NFC / А. С. Рабинович, О. В. Казарин. – Текст : непосредственный // Вестник Московского финансово-юридического университета. – 2015. – № 1. – С. 166–171.

6. Hill, Brian. Cisco: The Complete Reference / B. Hill. – McGraw-Hill Osborne Media, 2002. – 1300 p. – Text : direct.

7. Меньшенин, А. О. Защищенный протокол взаимодействия «хост – считыватель NFC» / А. О. Меньшенин, А. В. Кораблин. – Текст : непосредственный // Безопасность информационных технологий. – 2012. – № 2. – С. 72–76.