УДК 00 – вы ставите свой код

Кравченко С.С.

студент

Байкальский государственный университет

г. Иркутск, Российская Федерация

ПРОБЛЕМЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ И УСТРОЙСТВ В СИСТЕМЕ УМНОГО ДОМА

Аннотация: В настоящей статье рассматривается проблема аутентификации пользователей и устройств при формировании единой системы умного дома. IOT-платформы являются одним из наиболее актуальных и перспективных направлений в современных технологиях. Они позволяют предприятиям и организациям подключать и интегрировать различные устройства и системы в одну сеть, что позволяет им получать больше данных и информации для анализа и управления. Произведен анализ основных проблем аутентификации как пользователей, так и устройств.

Ключевые слова: Аутентификация, интернет вещей, умный дом

Kravchenko S.S.

Baikal State University,

Irkutsk, Russian Federation

The main problems of authentication of users and devices in the smart home system

Abstract. This article discusses about the problems of authenticating users and devices when forming a unified smart home system. IOT platforms are one of the most relevant and promising areas in modern technologies. They enable businesses and organizations to connect and integrate different devices and systems into one network, allowing them to gain more data and information for analysis and management. An analysis of the main problems of authentication of both users and devices was carried out.

Keywords. Authentication, Internet of things, smart home

Системы умного дома становятся все более популярными среди пользователей, обеспечивая им удобство, безопасность и энергоэффективность. Однако, с ростом популярности таких систем возникают проблемы с аутентификацией устройств и пользователей, которые могут привести к угрозам для безопасности и конфиденциальности.

Аутентификация – это процесс, при котором устройство и пользователь подтверждает подлинность своей личности в какой-либо системе. Система предоставляет личные данные только своему владельцу.

Механизмы аутентификации пользователей в системе умного дома обеспечивают безопасный доступ к функциям и устройствам системы, предотвращая несанкционированный доступ. Выделяют несколько распространенных механизмов аутентификации в системах умного дома:

- пароль или PIN-коды;
- биометрическая аутентификация;
- RFID и NFC метки;
- двухфакторная аутентификация;
- устройства аутентификации;
- геолокационная аутентификация;
- управление доступом по расписанию;
- цифровые сертификаты и ключи.

Устройство может предъявлять свои учетные данные для аутентификации в системе умного дома различными способами в зависимости от используемых технологий и протоколов. Вот несколько распространенных способов:

- уникальный идентификатор устройства;
- пароль или ключ доступа;
- сертификаты;
- токены доступа;
- одноразовые пароли или коды.

Аутентификация пользователей в системе умного дома имеет свои уникальные проблемы, которые важно учитывать для обеспечения безопасности и удобства использования. Вот некоторые из наиболее значимых проблем аутентификации пользователей:

– безопасность паролей, заключается в том, что пользователи могут использовать слабые пароли, которые легко поддаются взлому или перебору, либо пользователи могут использовать одни и те же пароли (так называемое переиспользование паролей) для нескольких сервисов, что увеличивает риск компрометации данных. Устанавливая же сложные пароли могут возникнуть трудности с их запоминанием, что может привести к их записыванию или использованию неэффективных методов для их хранения;

– управление биометрическими данными. Системы биометрической аутентификации могут быть не всегда точными и могут допускать ошибки как в положительном, так и в отрицательном направлении. В свою очередь хранение и обработка биометрических данных требует строгой защиты и соблюдения правил конфиденциальности, чтобы избежать утечек информации или злоупотребления;

– физические устройства аутентификации. Физические устройства аутентификации, такие как ключи или метки, могут быть потеряны или украдены, что приводит к потенциальным угрозам безопасности, а также устройства аутентификации могут быть не всегда надежными или могут выходить из строя, что может привести к проблемам доступа;

– двухфакторная аутентификация. Если пользователь меняет свой номер телефона без обновления информации в системе, это может привести к проблемам с получением одноразовых кодов по SMS. Злоумышленники могут создавать поддельные мобильные приложения для

перехвата одноразовых кодов, отправляемых для двухфакторной аутентификации;

− управление доступом. Если у пользователя нет возможности управлять своими учетными данными или правами доступа, это может привести к утечке данных или несанкционированному использованию;

− уязвимости устройств умного дома. Некоторые устройства умного дома могут иметь уязвимости в программном обеспечении или аппаратуре, которые могут быть использованы злоумышленниками для обхода механизмов аутентификации.

В целом, проблемы аутентификации устройств и пользователей в системе умного дома являются серьезной угрозой для безопасности и конфиденциальности. Поэтому необходимо принимать меры для защиты системы от несанкционированного доступа и обеспечить надежную аутентификацию устройств и пользователей.

Решение этих проблем требует сбалансированного подхода, включающего тщательное проектирование системы, обеспечение обучения пользователей вопросам безопасности и использование современных методов аутентификации и управления доступом.

Использованные источники:

1. Как защитить свой «Умный дом» от атаки? [Электронный ресурс] - URL: https://spark.ru/startup/hetmansoftware/blog/69238/kak-zaschitit-svoj-umnij-dom-ot-ataki (дата обращения: 01.02.2024)
2. Проблемы аутентификации и контроля доступа в системах «Умный дом» [Электронный ресурс] - URL: https://interactive-plus.ru/en/article/470219/discussion_platform (дата обращения: 01.02.2024)
3. Как защитить умный дом [Электронный ресурс] - URL: https://www.kaspersky.ru/blog/how-to-secure-smart-home/34849/ (дата обращения: 01.02.2024)

4. Криптография в системах умного дома [Электронный ресурс] - URL: https://nauchniestati.ru/spravka/zashhita-informaczii-v-sistemah-umnogo-doma/ (дата обращения: 01.02.2024)