УДК 004.056.5

Макушенко Д.Е. студент

5 курс, Донской государственный технический университет,

Россия, г. Ростов-на-Дону

ПРОЕКТИРОВАНИЕ МНОГОУРОВНЕВОЙ АРХИТЕКТУРЫ ЗАЩИТЫ ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ «УМНОГО ДОМА»

Аннотация. *В работе рассматривается проблема обеспечения доверенного обмена сообщениями в телекоммуникационных системах «умного дома», использующих протокол MQTT [1 с. 15; 4, с. 788]. Предложена архитектура разделения функций идентификации, контроля доступа и доставки сообщений, позволяющая устранить транзитивное доверие к брокеру. Выполнен сравнительный анализ базовой и расширенной моделей MQTT-взаимодействия с точки зрения структурной устойчивости и классов угроз.*

Ключевые слова: *MQTT, брокер сообщений, умный дом, модель доверия, архитектура безопасности, контроль доступа, распределённые системы.*

Abstract. *The paper addresses the problem of ensuring trusted message exchange in smart home telecommunication systems using the MQTT protocol [1 p. 15; 4, p. 788]. An architecture for separating the functions of identification, access control, and message delivery is proposed, which eliminates transitive trust in the broker. A comparative analysis of the basic and extended MQTT interaction models is performed from the perspective of structural resilience and threat classes.*

Keywords: *MQTT, message broker, smart home, trust model, security architecture, access control, distributed systems.*

Введение. Телекоммуникационные системы «умного дома» представляют собой распределённые среды взаимодействия большого числа устройств с ограниченными вычислительными ресурсами [2, с. 46]. Для организации обмена данными в таких системах широко применяется протокол MQTT, основанный на модели публикации и подписки.

Ключевым элементом архитектуры MQTT является брокер сообщений, выполняющий функции маршрутизации и доставки данных. Несмотря на логическую простоту данной модели, её использование приводит к формированию централизованной точки доверия, на которую опирается вся логика взаимодействия устройств [1, с. 18].

С точки зрения информационной безопасности это создаёт архитектурное противоречие: распределённая система взаимодействует через единый узел, принимающий решения о доставке сообщений, но не обладающий полноценной моделью верификации источников данных [3, с. 25].

Архитектура MQTT-взаимодействия представлена на рис. 1. Типовая система «умного дома» может быть представлена в виде трёх основных уровней: пользовательского уровня, уровня управления и уровня устройств [4, с 388].

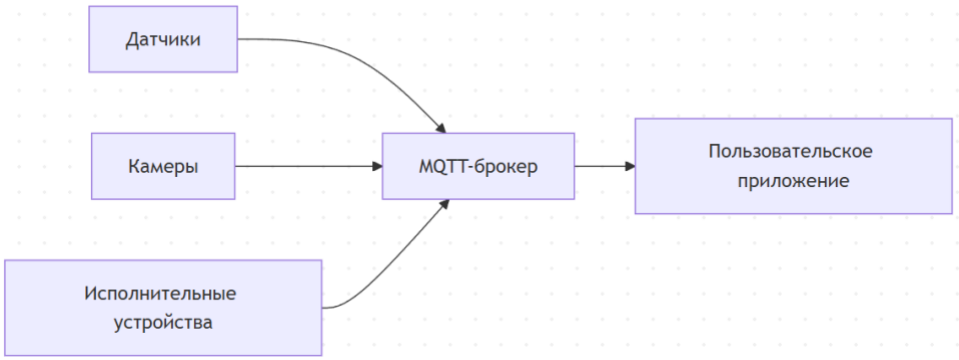

Рисунок 1. Базовая модель MQTT-взаимодействия

В данной модели брокер выполняет функцию единого посредника между всеми участниками обмена сообщениями. При этом семантика доверия к устройствам не разделяется на уровни, а сосредоточена в одном компоненте.

Архитектурные угрозы MQTT-систем. Безопасность MQTT-инфраструктуры определяется не отдельными уязвимостями, а структурой доверия между компонентами системы [6, с. 14]. Центральная проблема заключается в отсутствии явного разделения функций аутентификации и маршрутизации сообщений. Сравнительный анализ классов угроз, их причин и последствий представлен в таблице 1 [5, с. 53; 7, с. 197].

Таблица 1.

Механизмы защиты по уровням телекоммуникационной модели

Класс угрозы	Архитектурная причина	Последствие
Подмена участника	Отсутствие строгой идентификации клиентов	Нарушение доверенной идентичности
Подмена сообщений	Отсутствие криптографической привязки источника	Нарушение целостности управления
Повтор сообщений	Отсутствие контекстной уникальности сообщений	Нарушение логики событий
Централизация доверия	Брокер как единая точка принятия решений	Критическая точка отказа

Анализ показывает, что уязвимости MQTT носят системный характер и обусловлены архитектурной моделью взаимодействия компонентов, основанной на централизованном брокере сообщений [1, с. 20]. В отличие от протоколов с распределённой логикой верификации участников, MQTT переносит функции маршрутизации и косвенного управления доставкой сообщений в единый узел [6, с. 15]. Безопасность системы в такой конфигурации определяется не качеством отдельных реализаций, а структурой взаимодействия компонентов.

Ключевое ограничение MQTT проявляется в транзитивной модели доверия. Конечные устройства и клиентские приложения не обладают независимыми механизмами проверки источника сообщений и опираются на посредника, совмещающего инфраструктурные и логические функции. Компрометация брокера приводит к нарушению целостности всей системы

обмена сообщениями, поскольку отсутствуют альтернативные контуры верификации.

Повышение уровня безопасности MQTT рассматривается как переход от неявной модели доверия к архитектуре распределённого доверия с явным выделением контуров идентификации и авторизации. В этой конфигурации доверие перестаёт быть свойством транспортного уровня и переносится в отдельный слой управления идентичностями и политиками доступа.

Предлагаемая архитектура доверенного MQTT-взаимодействия. Предлагаемая архитектура доверенного MQTT-взаимодействия основана на декомпозиции функций на три независимых слоя: идентификация участников, управление доступом и доставка сообщений.

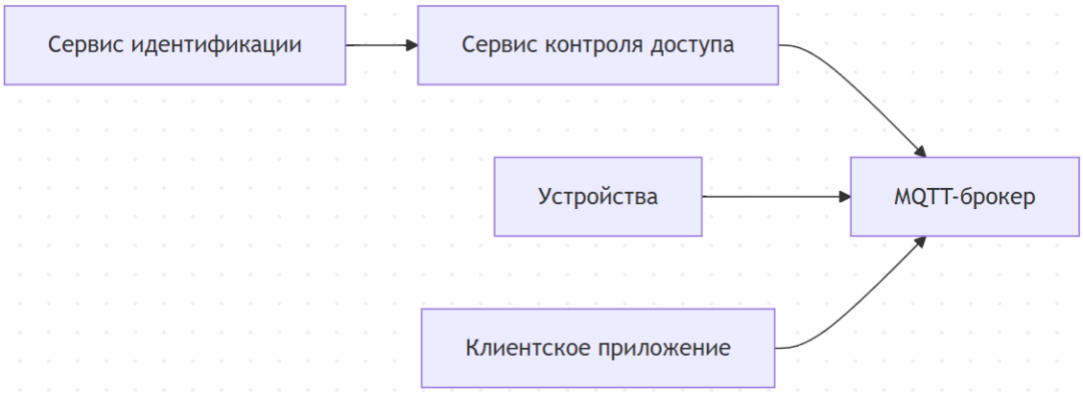

Рисунок 2. Архитектура разделённого доверия MQTT

В предложенной архитектуре брокер исключён из процесса принятия решений о доверии. Проверка идентичности и определение прав доступа выполняются внешними компонентами, формирующими независимый контур управления политиками безопасности.

Архитектурный переход от протокольно-центрированной модели к модели распределённого доверия изменяет основание безопасности системы: вместо параметров соединения определяющей становится структура взаимодействия и границы доверия между компонентами [7, с. 203].

Разделение функций идентификации и доставки сообщений приводит к следующим эффектам:

– устранение зависимости системы от брокера как единственной точки принятия решений о доступе;

– формализация политики доступа в отдельном логическом контуре;

– снижение последствий компрометации отдельных устройств за счёт изоляции доменов доверия;

– возможность независимого масштабирования подсистем идентификации и маршрутизации.

В рамках данной модели MQTT интерпретируется как транспортный механизм, функционирующий внутри распределённой архитектуры управления доверием, а не как самостоятельная доверенная среда.

Криптографическое обеспечение верификации источников сообщений. В предложенной архитектуре критическим элементом является механизм криптографической верификации источников сообщений, исключающий возможность подмены данных на транспортном уровне. Для реализации данного механизма применяется асимметричная криптография на основе эллиптических кривых (Elliptic Curve Cryptography, ECC), в частности алгоритм цифровой подписи ECDSA (Elliptic Curve Digital Signature Algorithm) [8, с. 5].

Выбор ECC обусловлен спецификой устройств «умного дома», характеризующихся ограниченными вычислительными ресурсами и энергопотреблением. В отличие от классических алгоритмов на основе RSA, ECC обеспечивает эквивалентный уровень криптографической стойкости при значительно меньшей длине ключа. Например, 256-битный ключ ECC обеспечивает стойкость, сопоставимую с 3072-битным ключом RSA, что критически важно для устройств с ограниченными ресурсами [8, с. 12].

Механизм верификации функционирует следующим образом:

– на этапе инициализации каждое устройство генерирует пару ключей (приватный и публичный). Приватный ключ хранится в защищенном хранилище устройства, публичный ключ регистрируется в сервисе управления идентификацией.

– при публикации сообщения устройство вычисляет хэш содержимого сообщения (используется алгоритм SHA-256) и формирует

цифровую подпись с использованием приватного ключа. Подпись добавляется к сообщению в виде дополнительного поля MQTT-пакета.

– на стороне сервиса контроля доступа (до передачи сообщения брокеру) выполняется верификация подписи с использованием зарегистрированного публичного ключа устройства. При успешной верификации сообщение помечается как доверенное и передается брокеру для маршрутизации. При неудачной верификации сообщение отклоняется, а инцидент регистрируется в системе мониторинга безопасности.

Заключение. В работе рассмотрена архитектура доверенного обмена сообщениями MQTT в системах «умного дома». Показано, что базовая модель MQTT формирует транзитивную структуру доверия, при которой брокер выступает единственным центром принятия решений о маршрутизации сообщений.

Предложенная архитектура разделяет функции идентификации, контроля доступа и доставки сообщений, что позволяет перейти к распределённой модели доверия и повысить структурную устойчивость системы к классу атак, связанных с подменой участников и несанкционированной публикацией сообщений.

Использованные источники

1. Дорофеев А.В., Марков А.С. Кибербезопасность умного дома: угрозы, модели, методы защиты / А.В. Дорофеев, А.С. Марков // Вопросы кибербезопасности. — 2022. — № 3 (49). — С. 15–28. — DOI: 10.21681/2311-3456-2022-3-15-28.

2. Statista Research Department. Number of IoT connected devices worldwide 2019–2030 [Электронный ресурс]. — URL: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (дата обращения: 12.04.2026).

3. IEC 62443-3-3:2013. Industrial communication networks — Network and system security. — Geneva : IEC, 2013. — 100 p.

4. Atzori L., Iera A., Morabito G. The internet of things: A survey / L. Atzori, A. Iera, G. Morabito // Computer Networks. — 2010. — Vol. 54, № 15. — P. 2787–2805. — DOI: 10.1016/j.comnet.2010.05.010.

5. OWASP IoT Top 10 2018 [Электронный ресурс]. — URL: https://owasp.org/www-project-internet-of-things/ (дата обращения: 15.03.2026).

6. Rose S., Borchert O., Mitchell S. Zero Trust Architecture : NIST SP 800-207 / S. Rose [et al.]. — Gaithersburg : NIST, 2020. — 50 p. — DOI: 10.6028/NIST.SP.800-207.

7. Shostack A. Threat Modeling: Designing for Security / A. Shostack. — Indianapolis : Wiley, 2014. — 624 p. — ISBN 978-1-118-80953-0.

8. Bernstein D.J., Lange T. Analysis and optimization of elliptic-curve single-scalar multiplication / D.J. Bernstein, T. Lange // Finite Fields and Applications. — 2007. — Vol. 461. — P. 1–19.