УДК 004.056

Миколаєнко В.В.
Салієва О.В.

РОЗРОБКА ЗАХИЩЕНОЇ АРХІТЕКТУРИ КОРПОРАТИВНОГО ВЕБ-МЕСЕНДЖЕРА З ВИКОРИСТАННЯМ МОДЕЛЮВАННЯ ЗАГРОЗ, TLS-ПРОТОКОЛУ ТА БЕЗПЕЧНОЇ WEBSOCET-ВЗАЄМОДІЇ

Вінницький Національний Технічний Університет

Анотація

Запропоновано захищену архітектуру корпоративного веб-месенджера з використанням моделювання загроз, протоколу TLS 1.3 та безпечної WebSocket-взаємодії. У роботі проведено аналіз сучасних моделей розгортання та архітектур корпоративних месенджерів, досліджено мережеві, прикладні та внутрішні загрози, а також виконано моделювання загроз за допомогою моделей STRIDE та DFD. На основі отриманих результатів спроєктовано мікросервісну архітектуру з API-шлюзом, окремими сервісами автентифікації, обміну повідомленнями та управління сесіями. Розроблено алгоритм взаємодії TLS-протоколу та WebSocket (WSS), який забезпечує конфіденційність, цілісність та доступність даних у режимі реального часу. Запропоноване рішення дозволяє суттєво підвищити рівень кіберзахисту корпоративних комунікацій при збереженні високої продуктивності системи.

Ключові слова: *корпоративний веб-месенджер, моделювання загроз, TLS 1.3, WebSocket, WSS, захищена архітектура, кібербезпека.*

Abstract

A secure architecture of a corporate web messenger using threat modeling, TLS 1.3 protocol, and secure WebSocket interaction is proposed. The paper analyzes modern deployment models and architectures of corporate messengers, investigates network, application, and internal threats, and performs threat modeling using STRIDE and DFD models. Based on the obtained results, a microservice architecture with an API gateway and separate authentication, messaging, and session management services is designed. An algorithm for the interaction of the TLS protocol and WebSocket (WSS) is developed, which ensures the confidentiality, integrity, and availability of data in real time. The proposed solution significantly increases the level of cybersecurity of corporate communications while maintaining high system performance.

Keywords: *corporate web messenger, threat modeling, TLS 1.3, WebSocket, WSS, secure architecture, cybersecurity.*

Вступ

У сучасних корпоративних середовищах веб-месенджери стали основним засобом оперативної комунікації, обміну конфіденційною інформацією та координації бізнес-процесів. Зростання обсягів оброблюваних даних і перехід на хмарні та гібридні моделі розгортання суттєво збільшили поверхню атаки таких систем. Захист корпоративних веб-комунікацій від мережевих, прикладних та внутрішніх загроз є критичним завданням, оскільки витік або компрометація інформації може призвести до значних фінансових втрат та порушення вимог нормативних документів у сфері кібербезпеки [1].

Існуючі рішення корпоративних месенджерів здебільшого зосереджені на базових механізмах автентифікації та шифрування, проте часто не забезпечують комплексного захисту на всіх рівнях архітектури. Традиційні підходи недостатньо враховують особливості реального часу обміну повідомленнями, а також специфіку взаємодії протоколів TLS та WebSocket у високонавантажених системах. Крім того, відсутність системного моделювання загроз на етапі проєктування знижує стійкість архітектури до сучасних кіберзагроз.

Перспективним напрямком підвищення захищеності є поєднання методів моделювання загроз з використанням сучасних криптографічних протоколів. У роботі проведено аналіз моделей розгортання та архітектур корпоративних веб-месенджерів, досліджено актуальні загрози та виконано моделювання

ризиків за допомогою підходів STRIDE та DFD. На основі отриманих результатів запропоновано захищену мікросервісну архітектуру з інтеграцією TLS 1.3 та безпечної WebSocket-взаємодії (WSS).

Метою роботи є проєктування захищеної архітектури корпоративного веб-месенджера та розробка алгоритму взаємодії протоколу TLS 1.3 з WebSocket, що забезпечить конфіденційність, цілісність та доступність даних при збереженні високої продуктивності системи.

Дослідження

У роботі проведено комплексний аналіз існуючих підходів до захисту корпоративних веб-месенджерів. Виконано класифікацію систем за моделями розгортання (хмарна, локальна, гібридна) та архітектурними рішеннями (клієнт-серверна та мікросервісна). Показано, що мікросервісна архітектура забезпечує кращу масштабованість, відмовостійкість та ізоляцію компонентів порівняно з монолітною клієнт-серверною моделлю.

Здійснено аналіз сучасних загроз для корпоративних веб-комунікацій, включаючи мережеві (MITM, DDoS, TLS downgrade), прикладні (XSS, CSRF, SQL-ін'єкції, WebSocket hijacking) та внутрішні загрози (компрометація облікових записів, інсайдерські дії). Для систематизації загроз застосовано модель STRIDE та побудовано DFD-діаграми потоків даних, що дозволило виявити критичні точки атаки та формалізувати ризики.

Виконано порівняльний аналіз протоколу TLS 1.3 та WebSocket. Показано переваги TLS 1.3 над попередньою версією за критеріями криптографічної стійкості, захисту від downgrade-атак, продуктивності (зменшення RTT з 2 до 1) та накладних витрат. Обґрунтовано доцільність використання захищеного з'єднання WSS (WebSocket over TLS 1.3) для обміну повідомленнями в реальному часі.

На основі результатів моделювання загроз запропоновано мікросервісну архітектуру корпоративного веб-месенджера, яка включає API-шлюз як єдину точку входу, окремі сервіси автентифікації, обміну повідомленнями, управління сесіями, логування та моделювання загроз. Така структура забезпечує принцип нульової довіри, мінімальні привілеї та ізоляцію компонентів.

Розроблено алгоритм взаємодії TLS-протоколу та безпечної WebSocket-взаємодії, який охоплює етапи встановлення TCP-з'єднання, виконання TLS 1.3 handshake, автентифікацію, ініціалізацію WSS-з'єднання, обмін повідомленнями в реальному часі та коректне завершення сесії. Алгоритм забезпечує конфіденційність, цілісність та доступність даних при збереженні високої продуктивності системи.

Висновок

У роботі запропоновано захищену архітектуру корпоративного веб-месенджера з використанням моделювання загроз, протоколу TLS 1.3 та безпечної WebSocket-взаємодії. Проведено аналіз моделей розгортання та архітектурних рішень корпоративних месенджерів, досліджено мережеві, прикладні та внутрішні загрози, а також виконано моделювання загроз за допомогою моделей STRIDE та DFD.

На основі отриманих результатів спроєктовано мікросервісну архітектуру з API-шлюзом як єдиною точкою входу, окремими сервісами автентифікації, обміну повідомленнями, управління сесіями та моделювання загроз. Розроблено алгоритм взаємодії TLS 1.3 та WebSocket (WSS), який забезпечує конфіденційність, цілісність та доступність даних у режимі реального часу.

Запропоноване рішення дозволяє суттєво підвищити рівень кіберзахисту корпоративних комунікацій при збереженні високої продуктивності системи. Отримані результати підтверджують ефективність комплексного підходу до проєктування захищених веб-месенджерів і створюють практичну основу для подальшої програмної реалізації та тестування системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. – Київ: ДП «УкрНДНЦ», 2023.
2. ДСТУ ISO/IEC 27002:2023. Інформаційні технології. Методи захисту. Кодекс практик щодо заходів інформаційної безпеки. – Київ: ДП «УкрНДНЦ», 2023.

3. ДСТУ ISO/IEC 27005:2022. Управління ризиками інформаційної безпеки. – Київ: ДП «УкрНДНЦ», 2022.
4. Закон України «Про основні засади забезпечення кібербезпеки України». – Відомості Верховної Ради України, ред. 2023 р.
5. Закон України «Про захист інформації в інформаційно-комунікаційних системах». – Відомості Верховної Ради України, ред. 2023 р.
6. Конахович Г.Ф., Клімушин П.С. Кібербезпека інформаційних систем: сучасні загрози та методи захисту. – Київ: КПІ ім. Ігоря Сікорського, 2021.
7. Литвиненко О.В. Захист веб-застосунків у корпоративних мережах. – Харків: ХНУРЕ, 2022.

Миколанєко Віталія Володимирівна – студентка групи 1КІТС-22б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: vitalinaaaa.m26098534@gmail.com

Салієва Ольга Володимирівна – доцент, Вінницький національний технічний університет, м. Вінниця.

Mykolanienko Vitaliia Volodymyrivna – student of Group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: vitalinaaaa.m26098534@gmail.com.

Saliieva Olha Volodymyrivna – Associate Professor, Vinnytsia National Technical University, Vinnytsia, Ukraine.