УДК 004.056

Б. М. Куцик
Ю. Є. Яремчук

ПРОТОКОЛ ІНІЦІАЛІЗАЦІЇ ЗАХИЩЕНОГО СЕАНСУ У ВЕБ-ДОДАТКАХ НА ОСНОВІ ВДОСКОНАЛЕНОГО ГІБРИДНОГО УЗГОДЖЕННЯ КЛЮЧІВ ТА МОДИФІКОВАНОЇ KDF

Вінницький національний технічний університет

Анотація

У роботі запропоновано протокол ініціалізації захищеного сеансу для веб-додатків, що поєднує вдосконалений метод гібридного узгодження ключів та модифіковану функцію формування ключів (KDF). Гібридний підхід забезпечує криптостійкість за рахунок комбінування класичного епізодичного узгодження (із властивістю forward secrecy) та додаткового компонента, орієнтованого на підвищення стійкості до сучасних і перспективних атак. Запропонована KDF передбачає жорстке прив'язування ключового матеріалу до контексту сеансу, параметрів протоколу та ролей сторін, що знижує ризики повторного використання ключів і атак пониження криптографічних параметрів. Сформульовано вимоги безпеки, наведено архітектуру протоколу та підхід до інтеграції у веб-середовище.

Ключові слова: захищений сеанс, веб-додатки, гібридне узгодження ключів, KDF, forward secrecy, стійкість до MITM, прив'язка до контексту.

Abstract

The paper proposes a secure session initialization protocol for web applications based on an improved hybrid key agreement method and a modified key derivation function (KDF). The hybrid approach combines a classical ephemeral agreement (providing forward secrecy) with an additional component aimed at strengthening resistance against both current and emerging attacks. The proposed KDF enforces strict binding of key material to the session context, protocol parameters, and party roles, reducing risks of key reuse and downgrade attacks. Security requirements, protocol architecture, and an integration approach for web environments are outlined.

Keywords: secure session, web applications, hybrid key agreement, KDF, forward secrecy, MITM resistance, context binding.

Вступ

Веб-додатки обробляють облікові дані, персональну інформацію та бізнес-критичні транзакції, тому етап ініціалізації сеансу є однією з ключових точок ризику. Попри широке застосування стандартних транспортних механізмів захисту, на практиці залишаються актуальними проблеми: коректне розділення ключів за призначенням, прив'язка ключового матеріалу до параметрів сеансу, стійкість до атак пониження криптографічних алгоритмів, повторного відтворення повідомлень та компрометації частини секретів.

Метою роботи є розробка протоколу ініціалізації захищеного сеансу у веб-додатках на основі вдосконаленого гібридного узгодження ключів і модифікованої KDF, що забезпечує криптографічну гнучкість, підвищену стійкість до атак на обмін ключами та коректне формування сімейства сеансових ключів для різних задач (шифрування, автентифікація, відновлення/продовження сеансу тощо).

Результати дослідження

У межах дослідження розроблено протокол ініціалізації захищеного сеансу у веб-додатках, у якому спільний ключовий матеріал формується через гібридне узгодження та контекстно-залежну KDF. Гібридний підхід розглядається як поєднання двох незалежних компонентів секретності: S1 – епізодичний класичний секрет із властивістю forward secrecy та S2 – додатковий секрет узгодження, який підсилює стійкість протоколу в разі компрометації частини секретів або зміни моделі загроз. Ключовий матеріал у запропонованій схемі не використовується напряму: отримані значення спочатку зводяться до єдиного входу Hybrid IKM (input keying material) і лише потім проходять стандартизовану двоетапну процедуру derivation типу Extract/Expand на основі HKDF [1]. Таке розділення дозволяє, з одного боку, отримати стабільний проміжний секретний стан, а з іншого – детерміновано сформувати сімейство похідних ключів за призначенням без ризику випадкового повторного використання ключового матеріалу.

Модифікація KDF у роботі зосереджена на коректному формуванні параметрів salt і info, а не на заміні криптопримітива. На етапі HKDF-Extract запропоновано жорстко прив'язувати результат до контексту рукостискання через salt, сформований на основі хешу транскрипту обміну, щоб будь-яка підміна параметрів узгодження або пониження криптографічного набору призводили до формування несумісних ключів і зриву встановлення сеансу. Подібний принцип використання транскрипту та HKDF-key schedule є характерним для сучасних сеансових протоколів, зокрема TLS 1.3 [2]. На етапі HKDF-Expand у info вводяться мітка призначення (label) і структурований контекст (роль сторони, погоджені параметри протоколу, ідентифікатор профілю/додатка), що реалізує domain separation та забезпечує незалежність ключів для різних криптографічних задач, узгоджуючись із рекомендаціями щодо деривації ключів у схемах встановлення ключів [3]. У результаті протокол отримує не один універсальний ключ, а керований набір похідних ключів із чіткою областю застосування та прогнозованим життєвим циклом.

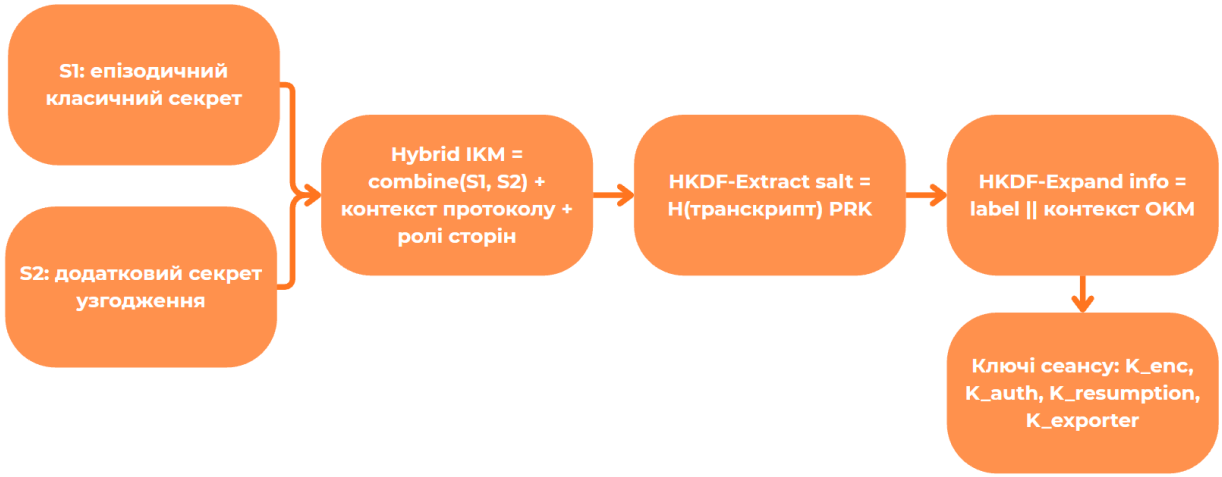

Рисунок 1 - Схема формування сеансових ключів у запропонованому протоколі (адаптовано за HKDF із модифікацією контексту та міток призначення).

Як показано на рис. 1, секрети S1 і S2 спочатку об'єднуються у Hybrid IKM разом із контекстом протоколу та ролями сторін, після чого виконується HKDF-Extract для отримання проміжного ключового стану PRK [1]. Далі HKDF-Expand формує кінцевий OKM, використовуючи info = label || контекст, завдяки чому окремі сеансові ключі для шифрування, автентифікації та відновлення/продовження сеансу є криптографічно розділеними й не можуть бути взаємозамінними навіть за збігу частини вхідних даних [3]. Практична перевага такого підходу для веб-середовища полягає в поєднанні forward secrecy з додатковою страховкою гібридного узгодження, а також у підвищенні надійності ініціалізації сеансу через прив'язку ключів до транскрипту та параметрів узгодження, що зменшує ризики MITM/downgrade-сценаріїв і некоректної повторної деривації ключів у різних контекстах [2].

Висновки

У роботі запропоновано протокол ініціалізації захищеного сеансу у веб-додатках на основі вдосконаленого гібридного узгодження ключів і модифікованої процедури формування сеансових ключів. Обґрунтовано використання двоетапної KDF Extract/Expand на базі HKDF для отримання проміжного ключового стану та подальшого виведення криптографічно розділеного набору ключів за призначенням із контекстним зв'язуванням до параметрів протоколу, ролей сторін і транскрипту обміну. Показано, що така організація ключового розкладу підвищує надійність встановлення сеансу, зменшує ризики повторного використання ключового матеріалу та посилює стійкість до атак пониження параметрів і підміни в процесі узгодження. Запропонований підхід може бути інтегрований у веб-середовище як прикладний механізм формування ключів для шифрування й автентифікації з можливістю подальшого розширення під конкретні вимоги захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. RFC 5869. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). IETF, 2010. [Електронний ресурс]. Режим доступу до ресурсу: https://datatracker.ietf.org/doc/html/rfc5869 (дата звернення 15.02.2026)

2 RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3. IETF, 2018. [Електронний ресурс]. Режим доступу до ресурсу: https://datatracker.ietf.org/doc/html/rfc8446 (дата звернення 15.02.2026).

3 NIST SP 800-56C Rev.1. Recommendation for Key-Derivation Methods in Key-Establishment Schemes. National Institute of Standards and Technology (NIST), 2018. [Електронний ресурс]. Режим доступу до ресурсуhttps://csrc.nist.gov/pubs/sp/800/56/c/r1/final (дата звернення 15.02.2026)

Куцик Богдан Михайлович – студент групи КІТС-22б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: mkkbodya@gmail.com

Kutsyk Bohdan M. – student of group KITS-22b, Faculty of Management and information security, Vinnytsia National Technical University, Vinnytsia, email: mkkbodya@gmail.com

Яремчук Юрій Євгенович – доктор технічних наук, професор, директор Центру ІТ та захисту інформації, сертифікований інструктор Мережевої Академії Cisco, Вінницький національний технічний університет, м. Вінниця.

Yaremchuk Yurii Yevhenovych – Doctor of Technical Sciences, Professor, Director of the IT and Information Protection Center, Certified Cisco Networking Academy Instructor, Vinnytsia National Technical University, Vinnytsia, Ukraine.