УДК 004.056.55

Волинець С.Ю.

Салієва О.В.

ПІДВИЩЕННЯ БЕЗПЕКИ ВЕБ-ЗАСТОСУНКІВ ШЛЯХОМ ІНТЕГРАЦІЇ ДОКАЗІВ З НУЛЬОВИМ РОЗГОЛОШЕННЯМ ZK-SNARK У ПРОТОКОЛ TLS 1.3

Вінницький національний технічний університет

Анотація

У роботі аналізуються недоліки традиційних механізмів автентифікації у веб-застосунках, що функціонують на базі захищеного протоколу TLS 1.3. Встановлено, що навіть за наявності шифрованого каналу, передача секретних даних (паролів, токенів) залишається основним вектором атак. Запропоновано удосконалений протокол, що інтегрує механізм автентифікації на основі доказів з нульовим розголошенням (zk-SNARK) одразу після встановлення сеансу за допомогою обміну ключами на еліптичних кривих (ECDHE). Такий підхід повністю виключає передачу облікових даних клієнта, значно підвищуючи стійкість до фішингу та компрометації серверних баз даних.

Ключові слова: TLS 1.3, автентифікація, докази з нульовим розголошенням, zk-SNARK, еліптична криптографія, безпека веб-застосунків.

Abstract

This paper analyzes the shortcomings of traditional authentication mechanisms in web applications operating over the secure TLS 1.3 protocol. It is established that even with an encrypted channel, the transmission of secret data (passwords, tokens) remains a primary attack vector. An improved protocol is proposed that integrates an authentication mechanism based on zero-knowledge proofs (zk-SNARK) immediately after session establishment via Elliptic Curve Diffie-Hellman (ECDHE) key exchange. This approach completely eliminates the transmission of client credentials, significantly increasing resistance to phishing and server database compromises.

Keywords: TLS 1.3, authentication, zero-knowledge proofs, zk-SNARK, elliptic curve cryptography, web application security.

Вступ

Протокол Transport Layer Security (TLS) версії 1.3 є сучасним стандартом для захисту комунікацій в Інтернеті [1]. Він забезпечує високий рівень безпеки каналу зв'язку завдяки використанню надійних криптографічних алгоритмів, зокрема, обов'язковому застосуванню механізмів обміну ключами на еліптичних кривих (ECDHE) для забезпечення досконалої прямої секретності. [2]. Це означає, що навіть у разі компрометації довгострокового ключа сервера, минулі сеанси зв'язку залишаться захищеними.

Однак, незважаючи на надійність шифрування на транспортному рівні, фундаментальна проблема залишається на рівні застосунку. Класичні методи автентифікації, такі як логін-пароль або API-токени, покладаються на передачу секретних даних від клієнта до сервера. Хоча ці дані шифруються, сам факт їх передачі створює ризики: компрометація бази даних на сервері призводить до масового витоку облікових даних, а користувачі залишаються вразливими до фішингових атак [3].Проблема полягає не в шифруванні, а в самій парадигмі автентифікації, яка базується на передачі секрету, а не на доведенні знання про нього.

Метою даної роботи є розробка та аналіз протоколу, що вирішує цю проблему шляхом інтеграції доказів з нульовим розголошенням (Zero-Knowledge Proofs, ZKP) у протокол TLS 1.3. Зокрема, пропонується використовувати компактні неінтерактивні докази zk-SNARK, які дозволяють користувачеві підтвердити знання свого пароля, не розкриваючи його [4].

Результати дослідження

Основою сучасних протоколів безпеки, включно з TLS 1.3, є криптографія на еліптичних кривих (ECC). Її головна перевага над традиційними алгоритмами, як-от RSA, полягає у значно вищій ефективності: ECC забезпечує еквівалентний рівень безпеки при суттєво менших розмірах ключів [2]. Наприклад, 256-бітний ключ ECC є настільки ж надійним, як 3072-бітний ключ RSA. Ця ефективність робить можливим впровадження додаткових, обчислювально складних механізмів безпеки, таких як ZKP, навіть на пристроях з обмеженими ресурсами.

Запропонований протокол складається з двох основних фаз, що виконуються в рамках одного з'єднання:

1. Встановлення захищеного каналу. На цьому етапі клієнт і сервер використовують стандартний механізм рукостискання TLS 1.3 з обміном ключами ECDHE. Результатом є створення повністю зашифрованого каналу зв'язку з досконалою прямою секретністю.

2. Автентифікація з нульовим розголошенням. Після встановлення каналу, замість традиційної відправки логіна та пароля, відбувається наступний процес:

2.1 Сервер надсилає клієнту унікальний одноразовий виклик (nonce).

2.2 Клієнтський застосунок, використовуючи пароль користувача та отриманий nonce, генерує криптографічний доказ zk-SNARK. Цей доказ математично підтверджує, що клієнт знає правильний пароль, але не містить жодної інформації про сам пароль [4].

2.3 Клієнт надсилає цей компактний доказ серверу.

2.4 Сервер перевіряє доказ. Успішна перевірка підтверджує особу користувача і дозволяє розпочати сеанс.

Головною перевагою такого підходу є те, що пароль користувача ніколи не залишає клієнтський пристрій і не передається мережею, навіть у зашифрованому вигляді. Це повністю усуває ризик перехоплення облікових даних та робить викрадені з сервера хеші паролів марними для зловмисників, оскільки вони не можуть бути використані для генерації доказу [3].

Водночас, основним недоліком є збільшення навантаження на клієнтський пристрій. Генерація доказу zk-SNARK є ресурсомісткою операцією і може займати від двох до п'яти секунд на сучасному обладнанні [5]. На противагу цьому, перевірка доказу на стороні сервера є дуже швидкою (кілька мілісекунд). Таким чином, виникає компроміс: значне підвищення безпеки досягається ціною прийнятної затримки під час входу користувача в систему.

Висновок

Інтеграція автентифікації на основі zk-SNARK у протокол TLS 1.3 дозволяє створити принципово новий рівень захисту для веб-застосунків. Усуваючи необхідність передачі паролів, запропонований підхід нейтралізує одні з найпоширеніших векторів атак, пов'язаних із крадіжкою облікових даних.

Ключовим результатом аналізу є виявлений компроміс між безпекою та продуктивністю. Хоча запропонований метод забезпечує безпрецедентний рівень захисту, він створює додаткове обчислювальне навантаження на клієнта, що призводить до затримки під час автентифікації. Для систем, що працюють з особливо чутливими даними (фінансові сервіси, медичні портали), така затримка є виправданою платою за кардинальне підвищення безпеки. Для менш критичних застосунків традиційні методи можуть залишатися прийнятними. Подальші дослідження можуть бути спрямовані на оптимізацію процесу генерації доказів для зменшення навантаження на клієнтські пристрої.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. The Transport Layer Security (TLS) Protocol Version 1.3 [Електронний ресурс] / E. Rescorla // IETF – 2018 – Режим доступу до ресурсу: https://datatracker.ietf.org/doc/html/rfc8446
2. Combining Elliptic Curve Cryptography, Zero-Knowledge Proofs, and Blockchain for Secure E-Voting Systems [Електронний ресурс] / A. Alharbi, A.M. Almuhaideb, M. Al-Ghamdi // International Journal of Innovative Research in Science and Services – 2024 – Режим доступу до ресурсу: https://www.ijirss.com/index.php/ijirss/article/view/9618
3. Zero Knowledge Authentication [Електронний ресурс] / Sedicii // sedicii.com – 2024 – Режим доступу до ресурсу: https://sedicii.com/news/zero-knowledge-authentication/
4. The knowledge complexity of interactive proof-systems [Електронний ресурс] / S. Goldwasser, S. Micali, C. Rackoff // ACM Digital Library – 1985 – Режим доступу до ресурсу: https://dl.acm.org/doi/10.1145/22145.22178
5. Evaluating the Efficiency of zk-SNARK, zk-STARK, and Bulletproof in Real-World Scenarios: A Benchmark Study [Електронний ресурс] / M. El-Hajj, B. Oude Roelink // MDPI Information – 2024 – Режим доступу до ресурсу: https://www.mdpi.com/2078-2489/15/8/463

Волинець Сергій Юрійович – студент групи 2КІТС-24М, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: datynford@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@vntu.edu.ua

Volynets Serhii Y. – student of 2KITS-24m group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: datynford@gmail.com

Supervisor*:* ***Saliieva Olha V.*** – Doctor of Philosophy (PhD) in specialty 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, email: salieva8257@ vntu.edu.ua