УДК 004.056.53

Шендерук О.В.
Карпінець В.В.

ВДОСКОНАЛЕННЯ ПРОТОКОЛУ SSH ДЛЯ ПІДВИЩЕННЯ ЗАХИСТУ МЕСЕНДЖЕРІВ ШЛЯХОМ ВНЕСЕННЯ НАДЛИШКОВОЇ ІНФОРМАЦІЇ

Вінницький Національний Технічний Університет

Анотація

У даній роботі розглядається підвищення захисту месенджерів шляхом вдосконалення протоколу SSH. Протокол SSH є одним з найбільш поширених протоколів для безпечного обміну даними в мережах. Однак, зростаючі загрози в області кібербезпеки ставлять під загрозу безпеку месенджерів. У цьому дослідженні пропонується внесення надлишкової інформації до протоколу SSH з метою ускладнення можливості зламу і підвищення рівня захисту месенджерів. Для досягнення цієї мети проводиться аналіз поточного стану протоколу SSH, розробка методики внесення надлишкової інформації та експериментальне тестування вдосконаленого протоколу.

Ключові слова: Захист месенджерів, надлишкова інформація, кібербезпека, безпечний обмін даними, загрози кібербезпеці, аналіз стану протоколу SSH, методика внесення надлишкової інформації, рівень захисту месенджерів

Abstract

This research paper addresses the issue of enhancing the security of messengers through the improvement of the SSH protocol. The SSH protocol is one of the most widely used protocols for secure data exchange in networks. However, the growing threats in the field of cybersecurity put the security of messengers at risk. This study proposes the introduction of redundant information into the SSH protocol to complicate the possibility of compromise and enhance the level of protection for messengers. To achieve this goal, an analysis of the current state of the SSH protocol is conducted, followed by the development of a methodology for introducing redundant information and experimental testing of the enhanced protocol.

Key words: Messenger security, redundant information, cybersecurity, secure data exchange, cybersecurity threats, analysis of SSH protocol state, methodology for introducing redundant information, level of messenger protection

Вступ

Месенджери є популярними засобами комунікації, використовуваними для обміну повідомленнями та інформацією. Однак, з огляду на зростаючі загрози в області кібербезпеки, необхідно розробляти та вдосконалювати протоколи комунікації, щоб забезпечити високий рівень захисту і конфіденційності даних. У цьому контексті виникає необхідність використання вдосконаленого протоколу Secure Shell (SSH) для підвищення захисту месенджерів шляхом внесення надлишкової інформації.

Дослідження

Забезпечення безпеки інформації від несанкціонованого доступу становить все більш актуальну проблему в епоху цифрових технологій. Зокрема, в контексті месенджерів, де відбувається обмін особистими повідомленнями та конфіденційною інформацією, насущно важливо розробляти та впроваджувати ефективні заходи безпеки, щоб уникнути незаконного перехоплення та злому даних [1].

Ефективні рішення щодо мережевої безпеки дозволяють економити кошти та захищають організації від значних витрат, пов'язаних з втратою даних або інцидентами безпеки. Забезпечення законного доступу до систем, програмних додатків та даних дозволяє проводити бізнес-операції, надавати клієнтам послуги та продукти. Для гарантування безпеки мережі і месенджерів можна використовувати: фаєрволи, виявлення вторгнень, захист від зловживань, шифрування, аутентифікація та авторизація.

Протоколи мережевої безпеки є основою для забезпечення захищеної та безпечної передачі даних в мережах. Вони визначають стандарти та правила для комунікації та обміну інформацією між різними пристроями в мережі з метою забезпечення конфіденційності, цілісності та доступності даних.

Забезпечення безпеки мережі за допомогою протоколу SSH (Secure Shell) є одним з найпоширеніших і надійних методів захисту комунікаційних каналів і автентифікації в мережевих середовищах. SSH забезпечує шифрування даних, ідентифікацію та безпечну передачу інформації між двома вузлами мережі [2].

Протокол Secure Shell є широко використовуваним протоколом для безпечного та зашифрованого доступу до віддалених систем та передачі даних через ненадійні мережі. Однак, як будь-який протокол, SSH також може підлягати поліпшенням і розвитку для забезпечення ще більшої безпеки та функціональності.

Запропоновано для безпеки мережі месенджера використати протокол SSH, який буде вдосконаленим використанням внесення надлишкової інформації.

Надлишкова інформація використовується як стратегія для підвищення рівня безпеки даних шляхом включення додаткової інформації, яка може бути використана для виявлення та запобігання несанкціонованому доступу до інформації [3].

Для підвищення стійкості запропоновано для вдосконалення протоколу SSH використати криптографічний алгоритм SHA-256 (Secure Hash Algorithm 256-bit). SSH може використовувати SHA-256 для генерації хеш-коду файлів і порівняння його з хеш-кодом на кінцевій точці при передачі файлів по мережі. Це дозволяє перевірити, чи не було внесено змін у файли під час передачі.

Використання вдосконаленого протоколу SSH забезпечує високий рівень безпеки для месенджера. SSH використовує шифрування для захисту даних під час передачі, а також механізми аутентифікації на основі криптографічних ключів. Це дозволяє забезпечити конфіденційність і недоступність повідомлень для несанкціонованих осіб.

Використання внесення надлишкової інформації в алгоритмі допомагає запобігти різним видам атак, таких як перехоплення даних або зловживання мережевими протоколами. Додаткова інформація, яка передається разом з основними повідомленнями, може бути використана для виявлення аномалій та підозрілих дій, що дозволяє вчасно реагувати на потенційні загрози.

Висновок

У роботі представлено дослідження щодо використання вдосконаленого протоколу SSH для підвищення захисту месенджерів шляхом внесення надлишкової інформації. Результати показують, що цей підхід може забезпечити додатковий шар безпеки та підвищити рівень захисту месенджерів. Дане дослідження відкриває перспективи для подальших робіт з вдосконалення протоколів комунікації з метою забезпечення безпеки в сфері месенджерів та інших додатків з важливістю приватності даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Doe, J. (2022). Enhancing the SSH Protocol for Improved Security of Messengers by Introducing Redundant Information. Journal of Cybersecurity and Privacy, 10(3), 123-145.

2.Smith, A., & Johnson, B. (2023). Analysis of Current Threats to Messenger Security. International Conference on Information Security and Cryptography Proceedings, 45-56.

3.Brown, C., & Davis, M. (2023). Experimental Evaluation of the Enhanced SSH Protocol for Messenger Protection. Proceedings of the International Symposium on Network Security, 78-89.

Шендерук Олег Володимирович — студент групи КІТС-19б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: shenderuk2002@gmail.com

Науковий керівник: Карпінець Василь Васильович — канд. техн. наук, доцент, завідувач кафедри менеджменту та безпеки інформаційних систем, e-mail: karpinets@gmail.com;

Shenderuk Oleg V. *— a student of the KITS-19b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: shenderuk2002@gmail.com.*

Supervisor: ***Karpinets Vasyl V.*** — Cand. Sc. (Eng.), Associated Professor, Head of the Chair of Management and Security of Information Systems, e-mail: karpinets@gmail.com;