УДК 004.891

Луканов М.В.
Карпінець В.В.

ПРИХОВАНІ КАНАЛИ ІНФОРМАЦІЯ НА ОСНОВІ МЕРЕЖЕВИХ ПРОТОКОЛІВ

Вінницький національний технічний університет

Анотація

У цьому дослідженні було проведено комплексний аналіз різних показників для визначення найбільш підходящого протоколу для створення прихованого каналу зв'язку. В результаті комплексного порівняння протоколів SRTP виявився оптимальним вибором створення захищеного прихованого каналу передачі інформації. Для реалізації цього прихованого каналу обрано WebRTC, що використовує SRTP для відеоконференцій і дзвінків. Запропонований підхід передбачає використання відеоповідомлення, переданого через WebRTC, в якості контейнера для приховування прихованих даних.

Ключові слова: *мережевий протокол, прихований канал зв'язку, передача даних, захист даних, передача у режимі реального часу, SRTP, WebRTC, алгоритм.*

Abstracts.

In this study, a comprehensive analysis of various indicators was conducted to determine the most suitable protocol for creating a covert communication channel. As a result of a comprehensive comparison of protocols, SRTP turned out to be the best choice for creating a secure covert channel for information transmission. WebRTC, which uses SRTP for video conferencing and calls, was chosen to implement this hidden channel. The proposed approach involves using a video message transmitted via WebRTC as a container for hiding hidden data.

Keywords*: network protocol, covert communication channel, data transmission, data protection, real-time transmission, SRTP, WebRTC, algorithm.*

Вступ

На сьогоднішній день передача, збереження та обробка великої кількості даних потребують надання надійного захисту. Найнебезпечніший процес роботи з даними є їх передавання. Під час передавання даних існують великі ризики їх підміни або модифікації. Для забезпечення надійності передавання даних використовують різні протоколи, що шифрують та захищають дані, але інколи навіть цього не достатньо. Як один з можливих методів захисту інформації при її передача є приховування наявності самої передачі важливої інформації. Тому було проведено дослідження протоколів передачі даних та на основі найкращого розроблено алгоритм для утворення прихованого каналу передавання інформації. Для дослідження було обрано протоколи SIP, RTP, SFTP, FTPS та SRTP.

Результати дослідження

Протоколи зв'язку в реальному часі та протоколи безпечної передачі файлів відіграють важливу роль у різних сценаріях зв'язку та передачі даних. SIP забезпечує передачу голосу та мультимедійних даних, RTP полегшує потокове передавання медіа в реальному часі, SFTP забезпечує безпечну передачу файлів через SSH, FTPS забезпечує безпечну передачу файлів за допомогою SSL/TLS, а SRTP забезпечує безпечну передачу мультимедійних даних у реальному часі. Ці протоколи пропонують основні функції та заходи безпеки для ефективного і захищеного спілкування та обміну даними.

У таблиці 1 представлено комплексне порівняння протоколів, що висвітлюються їхні різні аспекти та функціональні можливості. Вивчаючи такі фактори, як використання, передача даних у режимі реального часу, підтримувані типи даних, механізми захисту даних, складність реалізації та використання мережевих ресурсів, отримано цінну інформацію про унікальні особливості та можливості кожного протоколу.

Провівши комплексний порівняльний аналіз протоколів за різними показниками, очевидно, що SRTP (Secure Real-Time Transport Protocol) є найбільш оптимальним вибором створення захищеного прихованого каналу передачі інформації.

Таблиця 1 – Порівняльний аналіз протоколів передачі даних

Протокол	Використання	Передача даних у реальному часі	Підтримувані типи даних для передачі	Захист даних	Використання ресурсів мережі
SIP (за [1-2])	Заснування сесій	–	Голос, відео, повідомлення	Обмежена (залежно від додаткових заходів безпеки)	Мінімальне
RTP (за [3-4])	Передача медіа	+	Аудіо, відео	Обмежена (без додаткових заходів безпеки)	Мінімальне
SFTP (за [5-6])	Захищена передача файлів	–	Файли різного типу	Висока (шифрування, аутентифікація)	Середнє
FTPS (за [7-8])	Захищена передача файлів	–	Файли різного типу	Висока (шифрування, аутентифікація)	Високе
SRTP (за [9-10])	Захищена передача медіа	+	Аудіо, відео	Висока (аутентифікація, приватність, захист від повторення)	Середнє

Для побудови алгоритму утворення прихованого каналу було обрано WebRTC, що включає в себе протокол SRTP для передавання даних. WebRTC надає можливість встановити одноранговий, зашифрований зв’язок, що підвищить надійність прихованого каналу. Також він є дуже популярними рішенням для створення проведення відеоконференцій та інтернет дзвінків, що зробить передавання даних ще більш непомітнішим [11].

Сам алгоритм містить наступні кроки: Крок 1. Розділити інформацію на частини; Крок 2. Передати усі частини використовуючи WebRTC у правильному порядку; Крок 3. Зібрати частини докупи та отримати цілісну інформацію на іншій стороні.

Під час передавання найкраще використовувати впровадження інформації саме в відеосигнал, що передає WebRTC. Навіть якщо вдасться перехопити та розшифрувати відеосигнал, то це все одно буде виглядати як звичайний дзвінок, лише детально дослідивши його, можна буде зробити висновок про присутність або відсутність прихованої інформації. Для виконання такого завдання, потрібні спеціалісти, час та гроші, що робить використання приховування інформації в відео сигналі більш вигідним та доцільним ніж впровадження її в пакет SRTP.

Висновки

Отже, з огляду на загальний аналіз показників у дослідженні, включаючи: використання, передачу даних в режимі реального часу, підтримувані типи даних, захист даних, використання мережевих ресурсів і потенціал для прихованих каналів зв'язку, SRTP виявляється найбільш оптимальним протоколом для утворення прихованого каналу. Але для побудови самого каналу найкраще підходить WebRTC, що використовує SRTP для створення відеоконференцій та дзвінків. Через популярність та розповсюдженість його використання не викличе підозр наявності в ньому прихованого каналу передачі інформації. Також найоптимальнішим способом утворення такого каналу є використання відео повідомлення, що передається WebRTC, як контейнера для прихованих даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке протокол ініціації сеансу. *Metaswitch*. URL: https://www.metaswitch.com/knowledge-center/reference/what-is-session-initiation-protocol-sip (дата звернення: 16.05.2023).

2. Що таке протокол ініціації сеансу (SIP) і як він працює?. Nextiva Blog. URL: https://www.nextiva.com/blog/sip-protocol.html (дата звернення: 17.05.2023).

3. Транспортний протокол реального часу (RTP. ExtraHop: Cloud-Native Network Detection and Response. URL: https://www.extrahop.com/resources/protocols/rtp/ (дата звернення: 17.05.2023).

4. Транспортний протокол реального часу (RTP). Online Courses and eBooks Library. URL: https://www.tutorialspoint.com/real-time-transport-protocol-rtp (дата звернення: 17.05.2023).

5. Арампаціс А. Що таке безпечний протокол передачі файлів (SFTP) і як ним користуватися. Платформа управління ідентифікацією машин. URL: https://venafi.com/blog/what-secure-file-transfer-protocol-sftp-and-how-use-it/ (дата звернення: 17.05.2023).

6. Протокол передачі файлів SSH (SFTP): отримати клієнт і сервер SFTP. PAM-рішення, системи керування ключами, безпечна передача файлів | SSH. URL: https://www.ssh.com/academy/ssh/sftp-ssh-file-transfer-protocol (дата звернення: 17.05.2023).

7. FTPS протокол. Wikipedia. URL: https://en.wikipedia.org/wiki/FTPS (дата звернення: 17.05.2023).

8. Шифрування FTPS, SFTP і PGP: основні компоненти стратегії безпечної передачі файлів. Precisely. URL: https://www.precisely.com/blog/data-security/ftps-sftp-pgp-encryption-secure-file-transfer (дата звернення: 17.05.2023).

9. SRTP – безпечний транспортний протокол реального часу. 3CX. URL: https://www.3cx.com/voip/srtp/ (дата звернення: 17.05.2023).

10. Безпечний протокол реального часу. Techopedia. URL: https://www.techopedia.com/definition/16483/secure-real-time-protocol-secure-rtp-or-srtp (дата звернення: 17.05.2023).

11. WebRTC. WebRTC. URL: https://webrtc.org (дата звернення: 17.05.2023).

Луканов Максим Всеволодович – студент групи КІТС-19б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail

Науковий керівник: **Карпінець Василь Васильович** – к.т.н., доц. каф. МБІС

Lukanov Maksym V. – student of group KITS-19b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail

Scientific adviser: **Karpinets Vasyl V.** – Candidate of Technical Sciences, Associate Professor. MBIS.