УДК 004.728.5
К.О. Ярощук
Тернопільський національний технічний університет імені Івана Пулюя, Україна

РЕАЛІЗАЦІЯ ФУНКЦІЙ ТРАНСПОРТНОГО РІВНЯ МОДЕЛІ OSI В ПРОТОКОЛІ TLS

K.O. Yaroshchuk
IMPLEMENTATION OF OSI TRANSPORT LAYER FUNCTIONS IN THE TLS PROTOCOL

Транспортний рівень є четвертим, тобто центральним, в моделі OSI, що частково пояснює його особливу роль в організації роботи мереж: він відокремлює три нижчих рівня, реалізація функцій яких залежить від використовуваного обладнання, від трьох верхніх рівнів, які не мають такої властивості.

Транспортний рівень повинен забезпечити виконання наступних функцій: транспортування даних через мережу, встановлення, підтримку та ліквідацію віртуальних каналів та послідовність передавання повідомлень.

Вже розроблено і впроваджено велику кількість протоколів, але усі вони по-різному і в різному об’ємі реалізують функції транспортного рівня.

Transport Layer Security (TLS), наступник Secure Socket Layer, є популярним протоколом для забезпечення конфіденційності і цілісності зв'язку шляхом встановлення надійного приватного каналу між двома партнерами. TLS досягає своїх цілей безпеки за допомогою симетричної криптографії з унікальними ключами, що генеруються для кожного з'єднання і кодів аутентифікації повідомлень.

Даний протокол широко використовується в додатках, що працюють з мережею Інтернет. TLS використовує асиметричну криптографію для аутентифікації, симетричне шифрування для конфіденційності та коди автентичності повідомлень для збереження цілісності повідомлень.

Перед тим, як почати обмін даними через TLS, клієнт і сервер повинні узгодити параметри з'єднання, а саме: версію використовуваного протоколу, спосіб шифрування даних, а також перевірити сертифікати, якщо це необхідно. Схема початку з'єднання називається TLS Handshake. Варто відзначити, що частіше за все в TLS використовується обмін ключами по алгоритму RSA: клієнт генерує симетричний ключ, підписує його за допомогою відкритого ключа сервера і відправляє його на сервер. У свою чергу, на сервері ключ клієнта розшифровується за допомогою закритого ключа. Недоліком цієї системи є той факт, що ця ж пара служить і для аутентифікації сервера. Тому всі браузери під час активного з'єднання TLS віддають перевагу саме поєднанню алгоритму Діффі-Хеллмана і використанню тимчасових ключів.

Технологія TLS False Start, що є розширенням протоколу, дозволяє відправляти дані, коли TLS Handshake завершений лише частково. На відміну від відновлення сесії, вона дозволяє передавати дані при минулому сеансі зв'язку або при первинному встановленні з'єднання.

Таким чином, протокол TLS в повному обсязі реалізує функції транспортного рівня моделі OSI.