Швед Р.П., Ільєнко А.В., Кравчук І.А.

Національний авіаційний університет, м.Київ

ДОСЛІДЖЕННЯ СУЧАСНИХ ПРОТОКОЛІВ ОРГАНІЗАЦІЇ ЗАХИЩЕНОЇ ПЕРЕДАЧІ ДАНИХ

Резюме.

Захист інформації під час передачі даних стає важливим завданням в сучасному світі. Робочі станції конкретної організації можуть бути надійно захищені, але при передачі інформації за межі закритого від проникнення периметра ймовірність витоку підвищується. В більшості випадків використання недостатньо ефективних засобів захисту стає причиною втрати персональних даних громадян або даних підприємства чи організації які мають характер комерційної таємниці. В такому випадку доцільним вважається використання сучасних криптографічних методів для організації захищеної передачі даних.

Ключові слова:

TLS, SSL, криптографічні методи, протокол, OpenSSL.

Abstract.

Protecting information during data transmission is becoming an important task in today's world. Workstations of a particular organization can be reliably protected, but when transmitting information outside the closed perimeter, the probability of leakage increases. In most cases, the use of insufficiently effective means of protection causes the loss of personal data of citizens or data of enterprises or organizations that are in the nature of trade secrets. In this case, it is advisable to use modern cryptographic methods to organize secure data transmission.

Keywords:

TLS, SSL, cryptographic methods, protocol, OpenSSL.

Загалом інформаційні об'єкти передаються від людини до людини, між організаціями та їх філіями або через кордони за допомогою загальних телекомунікаційних каналів, захист яких часто не залежить від конкретного власника даних. До таких каналів може підключитися зловмисник і перехопити незахищений трафік. З боку держав мірою захисту ресурсів стає концепція впровадження суверенного Інтернету, з боку організацій - використання сучасних криптографічних засобів захисту та захищених протоколів передачі інформації.

Одним з рішень для організації захищеної передачі даних є використання різних криптографічних протоколів таких як SSL або TLS. Метою даної роботи є дослідження сучасних протоколів організації захищеної передачі даних.

Мережеві протоколи SSL і TLS є криптографічними протоколами, що забезпечують аутентифікацію і захист від несанкціонованого доступу, порушення цілісності переданих даних. Протоколи SSL та TLS потрібні для виключення можливості підміни ідентифікатора з боку клієнта або сервера та виключення можливості розкриття або спотворення даних. Для цього застосовуються шифрування каналу зв'язку і коди цілісності повідомлень, що забезпечує надійний метод аутентифікації,.

Протокол TLS являє собою криптографічний протокол що використовують для захищеної передачі даних між різними вузлами в мережі інтернет. Даний протокол знайшов застосування в VoIP-додатках, веб-браузерах, додатках для миттєвого обміну повідомленнями. TLS реалізований на специфікації SSL 3.0. Зараз існує чотири версії TLS, всі вони описані в RFC: TLS 1.0, TLS 1.1, TLS 1.2 і вийшла в 2018 році версія TLS 1.3. TLS 1.0 багато в чому повторює SSLv3, за винятком ряду деталей, які, втім, є дуже важливими. (В криптографічних протоколах деталі важливі як ні в яких

інших протоколах Інтернету.) Ключовою відмінністю TLS від SSL є наявність підтримки цілого ряду розширень, що дозволяють реалізувати сучасні методи захисту інформації. TLS 1.1 і 1.2 досить близькі до 1.0, але у версії 1.2 з'явилися помітні поліпшення, наприклад, використовується інша основа псевдослучайной функції і введена підтримка шифрів в режимі аутентифицированного шифрування.

Основними можливостями протоколу TLS є: використання ключа для перевірки коду аутентифікації повідомлення; повідомлення з підтвердженням зв'язку містить хеш всіх повідомлень, якими обмінювалися сторони; використання нумерації записів додатки із застосуванням MAC; застосування псевдовипадкової функції, яка розділяє вхідне повідомлення на 2 частини, кожна з яких обробляється різної хеш-функцією.

В протоколі TLS використовують наступні алгоритми: для симетричного шифрування RC4, Triple DES, SEED, IDEA; для перевірки автентичності ключів RSA, DSA, ECDSA; для хеш-функцій MD5, SHA і SHA-256/384.

Додатки здійснюють обмін записами, які зберігають в собі дані. Записи можуть бути стиснуті, доповнені, зашифровані або ж ідентифіковані. При цьому в кожного запису вказуються дані про довжину пакета і використовуваної версії TLS.

Загалом використання криптографії в протоколах SSL та TLS досить сильно зменшує швидкість роботи додатків , проте надає надійний захист передачі даних. Такий протокол майже не вимагає ніяких налаштувань з клієнтської сторони, вважаються найпоширенішими протоколами захисту в мережі інтернет.

Протокол TLS забезпечує надійний захист передачі даних проте для передачі особливо важливої інформації в великих організаціях або,

наприклад, на рівні безпеки країни використання одного протоколу не є доцільним. Одним з рішень даної проблеми є організація захищеного TLS-з'єднання засобами криптографічного пакету OpenSSL.

Використання OpenSSL передбачає в собі удосконалення протоколу TLS на рівні створення сертифікату та його закритого ключа під час встановлення з'єднання між сервером та клієнтом за допомогою деяких алгоритмів шифрування. До таких алгоритмів можна віднести RSA що базується на обчислювальній складності задачі факторизації великих цілих чисел або алгоритм ECDSA що використовує групи точок еліптичної кривої для створення електронно цифрового підпису.

Для аутентифікації і подальшого узгодження сеансового ключа сервера необхідні власні сертифікат і закритий ключ, а клієнту - сертифікат (або довірча ланцюжок сертифікатів) центру сертифікації, який сертифікував сервер. Якщо клієнт довіряє сертифікату центру сертифікації, то він може перевірити валідність сертифіката сервера. Після цієї перевірки клієнт може бути впевнений, що обмінюється даними саме з тим вузлом, за який себе видає сервер таким чином криптографічний пакет OpenSSL забезпечує додатковий рівень захисту при організації захищеної передачі даних.

Висновки.

TLS ставить собі за мету створення між двома вузлами мережі захищеного від прослуховування і підміни інформації каналу зв'язку, придатного для передачі довільних даних в обох напрямках, а також перевірку того, що обмін даними відбувається між саме тими вузлами, для яких канал і планувався. Таким чином протокол TLS відповідає за забезпечення конфіденційності, цілісності та автентичності з'єднання (аутентифікації).

Література:

1. Венедюхин А.К Ключи, шифры, сообщения: как работает TLS

2. Что такое TLS[Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/258285/

3. Защита сайта по протоколу TLS [Електронний ресурс] – Режим доступу до ресурсу: https://www.leaderssl.ru/articles/209-zaschita-sayta-po-protokolu-tls

4. What is TLS (Transport Layer Security) [Електронний ресурс] – Режим доступу до ресурсу: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

5. OpenSSl [Електронний ресурс] – Режим доступу до ресурсу: https://www.openssl.org