Горецький О.А., магістрант,
Науковий керівник – Кубрак Ю.О., к.т.н, доц.,
Житомирський державний технологічний університет

БЕЗПЕКА ЕЛЕКТРОННОЇ КОМЕРЦІЇ НА ОСНОВІ ПРОТОКОЛУ TSL

Протокол TLS (transport layer security) заснований на протоколі SSL (Secure Sockets Layer), який спочатку був розроблений для підвищення безпеки електронної комерції в Інтернеті. Протокол SSL реалізований на application-рівні, безпосередньо над TCP (Transmission Control Protocol), що дозволяє більш високорівневим протоколам (таким як HTTP або протокол електронної пошти) працювати без змін. Якщо SSL налаштований коректно, то сторонній спостерігач може дізнатися лише параметри з'єднання (наприклад, тип використовуваного шифрування), а також частоту пересилання і приблизну кількість даних, але не може читати і змінювати їх.

Протокол TLS призначений для надання трьох послуг всім додаткам, які працюють над ним, а саме: шифрування, аутентифікація і цілісність. Технічно, не всі три можуть використовуватися, однак на практиці, для забезпечення безпеки, як правило використовуються всі три:

• Шифрування - приховування інформації, переданої від одного комп'ютера до іншого;
• Аутентифікація - перевірка авторства переданої інформації;
• Цілісність - виявлення підміни інформації підробкою.

Для того щоб встановити криптографічно безпечний канал даних, вузли з'єднання повинні узгодити використовувані методи шифрування і ключі. Протокол TLS однозначно визначає цю процедуру - TLS Handshake. Слід зазначити, що TLS використовує криптографію з відкритим ключем, яка дозволяє вузлам встановити загальний секретний ключ шифрування без будь-яких попередніх знань один про одного. Також в рамках процедури TLS Handshake є можливість встановити справжність особистості і клієнта, і сервера. Наприклад, клієнт може бути впевнений, що сервер, які надає йому інформацію про банківський рахунок, дійсно банківський сервер. І навпаки: сервер компанії може бути впевнений, що клієнт, який підключився до нього - саме співробітник компанії, а не є сторонньою особою (даний механізм називається Chain of Trust). Нарешті, TLS забезпечує відправку кожного повідомлення з кодом MAC (Message Authentication Code), алгоритм створення якого - одностороння криптографічна функція хешування (фактично - контрольна сума), ключі якої відомі обом учасникам зв'язку. Будь-який раз при відправленні повідомлення, генерується його MAC-значення, яке може згенерувати і приймач, це забезпечує цілісність інформації та захист від її підміни.

Таким чином, коротко розглянуті всі три механізми, що лежать в основі кріптобезопасності протоколу TLS.

За різними історичними і комерційних причин найчастіше 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. Після цього обмін ключами оголошується завершеним. Даний алгоритм має один недолік: ця ж пара відритого і закритого ключів використовується і для аутентифікації сервера. Відповідно, якщо зловмисник отримує доступ до закритого ключа сервера, він може розшифрувати весь сеанс зв'язку. Більш того, зловмисник може просто записати весь сеанс зв'язку в зашифрованому вигляді і зайняти розшифровкою потім, коли вдасться отримати закритий ключ сервера. У той же час, обмін ключами Діффі-Хеллмана видається більш захищеним, так як встановлений симетричний ключ ніколи не залишає клієнта або сервера і, відповідно, не може бути перехоплений зловмисником, навіть якщо той знає закритий ключ сервера. На цьому заснована служба зниження ризику минулих сеансів зв'язку: для кожного нового сеансу зв'язку створюється новий, так званий «тимчасовий» симетричний ключ. Відповідно, навіть в гіршому випадку (якщо зловмиснику відомий закритий ключ сервера), він може лише отримати ключі від майбутніх сесій, але не розшифрувати раніше записані.

Для отримання ще більшої швидкодії була розроблена технологія TLS False Start, що є опціональним розширенням протоколу і дозволяє відправляти дані, коли TLS Handshake завершена лише частково. Природно, виникають випадки, коли вже виданий сертифікат необхідно відкликати або анулювати (наприклад, був скомпрометований закритий ключ сертифіката, або була скомпрометована вся процедура сертифікації). Для цього сертифікати справжності містять спеціальні інструкції про перевірку їх актуальності. Отже, при побудові ланцюжка довіри, необхідно перевіряти актуальність кожного довірчого вузла. Механізм цієї перевірки простий і в його основі лежить «Список відкликаних сертифікатів» (CRL - «Certificate Revocation List»).

Отже протокол TLS є одним з протоколів який забезпечує цілісність, конфеденційність та захищенність передачі даних в наш час.