ПРОТОКОЛ БЕЗПЕКИ TLS

Битян О. І.
Чернівецький національний університет імені Юрія Федьковича, м. Чернівці

Ми використовуємо різні протоколи для забезпечення інформаційної безпеки в комп'ютерних мережах. Для криптографічної безпеки інформації часто використовується SSL / TLS (Secure Socket Layer / Transport Layer Security). Він розроблений компанією Netscape Communications. SSL / TLS спрямований на захист інформації, що передається між клієнтом і сервером комп'ютерної мережі. SSL став стандартом безпеки в Інтернеті через його переваги.

Цілями TLS є наступні (у порядку пріоритету):

1. Криптографічна безпека. TLS має використовуватися для безпечного з'єднання між двома партнерами.

2. Сумісність. Різні програмісти повинні вміти розробляти програми, які використовують TLS і зможуть успішно обмінюватися криптографічними параметрами, не знаючи прикладних можливостей один одного.

3. Розширюваність.

4. Відносна ефективність. Криптографічні операції потребують великої потужності процесора. Тому TLS має додаткову схему хешування сеансу. Це дозволяє зменшити кількість з'єднань, які використовують тимчасові буфери. Крім того, мережева активність була зменшена за рахунок певних заходів.

Алгоритми, які використовуються в TLS, можуть бути різними, залежно від версії протоколу. Є основні:

• для обміну ключами та його аутентифікації - використовуються RSA (асиметричний алгоритм), Diffie-Hellman (безпечний обмін ключами) або DSA (алгоритм цифрового підпису);

• Для симетричного шифрування - RC2, RC4, IDEA, DES, Triple DES або AES;

• Для хеш використовуються MD5 або SHA.

Починаючи з SSL 3.0 набір криптографічних алгоритмів був розширений (TLS 1.0 має дуже мало відмінностей від SSL 3.0, але вони не сумісні). Для аутентифікації взаємодіючих цифрових сертифікатів використовуються відкриті ключі, які відповідають стандарту x.509. Основою протоколу є технологія комплексного використання асиметричних і симетричних криптосистем. Він забезпечує безпечне підключення клієнт-сервер.

Література:

1. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

2. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков – К. : Видавнича група BHV, 2009. – 608 с.