УДК 621.319

АНАЛІЗ ПРОТОКОЛУ OTR ШИФРУВАННЯ ДЛЯ ОБМІНУ МИТТЄВИМИ ПОВІДОМЛЕННЯМИ

Пилипенко Б.В., Голь В.Д., Правило В.В.
Державний заклад Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ», Україна
E-mail: *dens1087@bk.ru*

Analysis protocol otr encryption for instant messaging

This paper analyzes the encryption method for instant messaging protocol XMPP / Jabber. An interaction procedures correspondents in the application of this method.

В роботі проведено аналіз методу шифрування OTR, який використовується в програмних продуктах, призначених для обміну миттєвими повідомленнями, визначені його переваги та недоліки, запропоновані принципи функціонування.

Характерними складовими методу є: обмін ключам, аутентифікація абонентів, шифрування та перевірка справжності протилежної сторони.

Обмін ключами

OTR використовує протокол Діффі-Хеллмана для обміну ключами, який є першим практичним методом для отримання загального секретного ключа при спілкуванні через незахищений канал зв'язку.

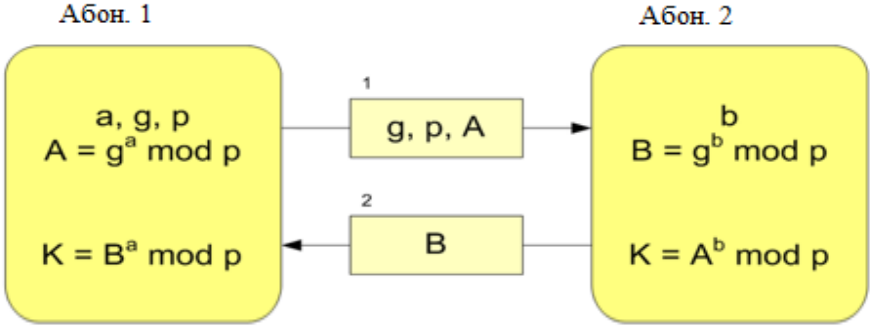

Рис. 1. Обмін таємними ключами.

При роботі алгоритму (рис. 1):

1. Кожна сторона генерує випадкове натуральне число a (b) – закритий ключ.

2. Спільно сторони встановлюють відкриті параметри p і g (зазвичай значення p і g генеруються на одній стороні і передаються іншій), де:

- p – є випадковим простим числом;

- g – є первісним коренем за модулем p (число g не повинно бути великим і зазвичай має значення в межах першого десятка).

3. Кожна сторона обчислює відкритий ключ A (B), використовуючи перетворення над закритим ключем:

$$A = g^a \bmod p; \quad B = g^b \bmod p.$$

4. Сторони обмінюються відкритими ключами з віддаленою стороною.

5. Кожна сторона обчислює загальний таємний ключ K, використовуючи відкритий ключ віддаленої сторони і свій закритий ключ:

$$K = B^a \bmod p; \quad K = A^b \bmod p.$$

K виходить рівним з обох сторін, тому що виконується властивість транзистивності:

$$B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = A^b \bmod p.$$

Аутентифікація.

Для цифрових підписів в OTR використовується алгоритм RSA, адже без додаткових засобів аутентифікації користувачі не могли бути впевнені, з ким саме вони згенерували загальний секретний ключ.

Рис. 1 Алгоритм аутентифікації абонентів.

Для відправника алгоритм аутентифікації буде наступним (рис. 2):

- взяти відкритий текст m;
- створити цифровий підпис s за допомогою свого секретного ключа {d, n}:

$$s = S_a(m) = m^d \bmod n$$

- передати пару {m, s}, що складається з повідомлення і підписи.

Для одержувача алгоритм аутентифікації складається з:

- приймання пари {m, s};
- приймання відкритого ключа {e} від відправника;
- обчислення прообразу повідомлення з підпису:

$$m' = P_s(s) = s^e \bmod e$$

- перевірки справжності підпису (незмінності повідомлення), порівнянням m і m'.

Шифрування.

Для шифрування в OTR застосований блоковий шифр AES. Цей алгоритм добре проаналізований і зараз широко використовується, будучи одним з найпоширеніших алгоритмів симетричного шифрування, оскільки 128-бітове шифрування AES наразі є досить надійним.

Перевірка справжності протилежної сторони.

Протокол Socialist Millionaire Protocol (SMP) використовується в OTR для

перевірки справжності протилежної сторони, знаючи якусь загальну таємницю. Даний протокол дозволяє упевнитися в тому, що учасники знають якусь загальну інформацію (пароль, відповідь на питання відома тільки їм) не розголошуючи її напряму, не обмінюючись якимись її ознаками, що можуть бути використані сторонньою людиною, що знаходиться нібито в середині системи. Man in the middle, MITM-атака – ситуація, коли сторонній (атакуючий) здатний читати і видозмінювати по своїй волі повідомлення, якими обмінюються кореспонденти, причому жоден з останніх не може здогадатися про його присутності в каналі (рис. 3).

Рис. 2. MITM-атака.

OTR використовує SMP для порівняння інформації двох учасників – ідентифікаторів сесії, які представляють собою відбитки публічних ключів учасників і власне самої «таємниці».

Отже виходячи з вище описаного, метод OTR шифрування дає досить високу надійність, так як обмін ключами відбувається за допомогою протоколу Діффі-Хеллмана, внаслідок чого отримується загальний таємний ключ при використанні відкритого каналу передачі. Також застосовується алгоритм аутентифікації абонента та використовується досить стійкий алгоритм шифрування і виконується перевірка справжності протилежної сторони. Але зазначений метод має суттєвий недолік, а саме, він є вразливим до MITM-атак, за допомогою яких можна скомпрометувати сервер, через який проходять повідомлення і таким чином получити доступ до переписки. Боротьба с цим недоліком можлива шляхом створення власного сертифікаційного центру (серверу), який буде видавати відкриті ключі для аутентифікації та здійснювати інші процедури, що пов’язані із використанням спільної (публічної) інформації.

Таким чином, можна вважати, що метод OTR шифрування є досить надійним і можливим для використання в відкритому програмному забезпеченні для захищеного обміну миттєвими повідомленнями, але за умови використання власного сертифікаційного центру (серверу). В інших випадках є ризик того, що до переписки буде наданий доступ стороннім особам.

Література

1. OTR шифрування [електроний ресурс]: https://habrahabr.ru/post/149591.
2. Енциклопедія OTR шифрування [електроний ресурс] : http://jabberworld.info/OTR.