насьогоднішній день. Наприклад: INSERT INTO t VALUES (1, AES_ENCRYPT ('text','password')) [2].

Використання вижче наведених способів дасть змогу значно покарщити захищеныcть БД MySQL.

Література

4. Захищаємо MySQL. Крок за кроком. [Електронний ресурс]. Режим доступу з http://www.securitylab.ru/analytics/216298.php.

5. Правильні способи захистити дані в таблицях БД. [Електронний ресурс]. Режим доступу з https://xakep.ru/2009/06/02/48406/

6. Справочное руководство по MySQL. [Електронний ресурс]. Режим доступу з http://www.mysql.ru/docs/man/Security.html

Войтович, В.С., Гриник Р.О.
Львівський державний університет безпеки життєдіяльності, м. Львів

ДОСЛІДЖЕННЯ НАДІЙНОСТІ ВИКОРИСТАННЯ ПРОТОКОЛУ IPSEC ДЛЯ СТВОРЕННЯ VPN

У сучасному світі різні VPN-технології використовуються повсюдно. Деякі як приклад, PPTP, з часом підтверджуються небезпечними і поволі втрачають чинність, інші навпаки, з кожним роком посилюють оберти. Але незмінним лідером і найбільш популярною технологією для створення і підтримки захищених приватних каналів як і раніше залишається IPsec VPN.

IPsec існує у вигляді розширення протоколу IPv4 і є невіднятою частиною IPv6. Даний протокол забезпечує безпеку IP-рівня мережі, що санкціонує постачання високого рівня захисту, прозорий для більшості служб, додатків і протоколів верхнього рівня, які використовують в якості транспорту протокол IP. IPSec не вимагає внесення змін в існуючі програми або операційні системи. Запровадження безпеки на даному рівні забезпечує захист для всіх протоколів сімейства TCP/IP, починаючи з рівня IP, таких як TCP, UDP, ICMP, а також безлічі інших.

Гарантії цілісності і конфіденційності даних в специфікації протоколу IPsec постачаються за рахунок використання механізмів аутентифікації і шифрування. Специфікація протоколу IPsec

обумовлює можливість підтримки зусиллями сторін інформаційного обміну багатоманітних протоколів та параметрів аутентифікації і шифрування пакетів даних, а також усіляких схем розподілу ключів. У той час результатом узгодження контексту безпеки є прилаштування індексу параметрів безпеки (SPI), що являє собою покажчик на конкретний елемент внутрішньої структури сторони інформаційного обміну, що відтворює можливі набори параметрів безпеки.

Концепція "захищеного віртуального з'єднання" є фундаментальною в архітектурі IPsec. "Захищене віртуальне з'єднання" – це симплексне з'єднання, яке формується для транспортування по ньому відповідного трафіку. Фундаментом використання протоколів AH або ESP (або обох одночасно) є реалізація послуг безпеки.

Всі види атак на компоненти IPSec можна диференціювати наступні підгрупи: атаки різновиду "Відмова в обслуговуванні, атаки, що використовують особливості і помилки конкретної реалізації IPSec і атаки засновані на уразливостях самих протоколів AH і ESP. Досліджуючи надійність протоколу до криптографічних атак слід звернути увагу на роботу Нільсона Фергюсона і Брюса Шнайера "Криптографічна оцінка IPSec" у якій вони відзначають, що виявили серйозні проблеми безпеки практично в усіх головних компонентах IPsec. Ці автори також зазначають, що набір протоколів вимагає серйозного доопрацювання для того, щоб він забезпечував хороший рівень безпеки.

Аналізуючи вище сказане можна зробити висновок, що протокол IPSec – це відкрита модульна платформа, що забезпечує більшу гнучкість для компаній, що обрали цю технологію. Значною перевагою IPSec являється те, що він працює на будь-якому виробнику, підтримує IPSec RFC, використання IPSec вирішує проблеми сумісності. Те, що IPSec є відкритим стандартом і працює на третьому рівні, дозволяє йому вирішувати більш складні завдання. Даний протокол є домінуючим серед усіх інших протоколів захисту передачі даних по мережі, але безпосередньо не є ідеальним і має ряд недоліків.

Література

1. DAVIS, Carlton R. IPSec: Securing VPNs. McGraw-Hill Professional, 2001.

2. LI, Zhitang; CUI, Xue; CHEN, Lin. Analysis and classification of ipsec security policy conflicts. In: Frontier of Computer Science and Technology, 2006. FCST'06. Japan-China Joint Workshop on. IEEE, 2006. p. 83-88.

3. FERGUSON, Niels; SCHNEIER, Bruce. A cryptographic evaluation of IPsec. Counterpane Internet Security, Inc, 2000, 3031: 14.

Косиєв О.А., Гриник Р.О.
Львівський державний університет безпеки життєдіяльності, м. Львів

АНАЛІЗ ВРАЗЛИВОСТЕЙ ЗАХИЩЕНОГО ПРОТОКОЛУ ПЕРЕДАЧІ ДАНИХ HTTPS

HTTPS протокол це протокол HTTP з додатковим шифруванням і автентифікацією між HTTP і TCP, які відбуваються через SSL або TSL, що гарантує захист від перехоплення інформації та від деяких атак [1].

Але не зважаючи на захист все ж існують способи отримання несанкціонованого доступу до інформації, що передається каналами зв'язку завдяки декільком найпоширенішим видам атак.

Атака за словником. Такий тип атак проводиться, коли атакуючий має уявлення про те, якого типу повідомлення надсилаються. Криптоаналітик може сформувати базу даних, де ключами є зашифровані рядки відкритого тексту. По створеній базі даних можна визначити ключ сесії, що відповідає певному блоку даних. Загалом для SSL такі атаки можливі. Але SSL намагається протистояти цим атакам, використовуючи великі ключі сесії – клієнт генерує ключ, який довший, ніж допускається експортними обмеженнями, частина якого посилається серверу відкритим текстом, а інша частина об'єднується з секретною частиною, щоб отримати достатньо довгий ключ (наприклад, 128 біт, як цього вимагає RC4). Спосіб блокування атак відкритого тексту полягає в тому, щоб зробити обсяг необхідного тексту неприйнятно великим. Кожен біт, що додається до довжини ключа сесії, збільшує розмір словника в 2 рази. Інший спосіб, за допомогою якого SSL може протистояти цій атаці, полягає в використанні максимально можливих довжин ключів (в разі не експортного варіанту). Наслідком цього є те, що найбільш