УДК 004.027

Т.О. Савчук[1]
О.О. Чернобай[1]

ЗАСТОСУВАННЯ ШИФРУВАННЯ ВЕРНАМА ДЛЯ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ НА ВЕБ-САЙТАХ З ВИКОРИСТАННЯМ СИСТЕМ УПРАВЛІННЯ БАЗАМИ ДАНИХ

[1] Вінницький національний технічний університет

Анотація

У доповіді запропоновано підхід до найбільш точного застосування принципів шифрування Вернама для захисту конфіденційних даних на веб-сайтах з використанням системи управління базами даних, що дозволяє скоротити зашифрованих даних при наявності типових переваг даної системи шифрування.

Ключові слова: шифр Вернама, принципи шифрування, криптографічна стійкість, база даних, зберігання ключа

Abstract

The report proposes an approach to the most precise application of the Vernam encryption principles to protect confidential data on websites using a database management system that reduces encrypted data in the presence of typical advantages of this encryption system.

Keywords: Vernam cipher, ciphering principles, cryptographic stability, database, key store

Вступ

Шифр Вернама – система симетричного шифрування, яка була запропонована в 1917 році співробітником AT&T Гільбертом Вернамом [1], та яка використовувала логічну операцію «Виключне АБО», або XOR, для шифрування повідомлення ключем. Особливістю такої системи є можливість дешифрування повідомлення застосуванням того ж алгоритму, який застосовувася для шифрування. В 1945 році американським криптоаналітиком Клодом Шенноном було доведено абсолютну криптографічну стійкість шифру Вернама у праці «Математична теорія криптографії».

Криптографічно стійке шифрування Вернама повинно відповідати таким вимогам, або принципам [2]:

- довжина ключа повинна співпадати з довжиною повідомлення, причому ніяка символьна послідовність в ключі не повинна повторюватись;
- заборонено шифрувати різні повідомлення одним і тим же ключем;
- ключ повинен генеруватися за допомогою випадкового рівномірного розподілу: P_k (k) = $1/2^N$, де k – ключ, N – кількість бінарних символів в ключі;
- після одного циклу шифрування/дешифрування ключ знищується з заміною на новий.

Аналіз проблеми

Задача генерування випадкових ключів шифрування та знищення використаних ключів в режимі реального часу була визнана складною ще на початку впровадження шифрування Вернама в комерційне використання. Тому для своїх апаратів Вернам застосовував закільцьовані рядки з ключами, заснованими на взаємно простих періодах [1]. Пізніше стали використовувати шифроблокноти з наперед визначеним набором ключів шифрування, доступ до яких повинні були мати лише відправник та отримувач повідомлення. В наш час шифрування Вернама зазвичай використовується державними структурами для захисту особливо важливих ліній зв’язку з відносно невеликим об’ємом даних.

Для сучасних веб-технологій з системами управління базами даних існують такі проблеми реалізації шифрування Вернама для захисту конфіденційних даних:

- ключ повинен генеруватися за допомогою випадкового рівномірного розподілу, для чого необхідно використовувати апаратні засоби генерації випадкових чисел, які за визначенням не можуть працювати в режимі реального часу, а отримувані за допомогою алгоритмічних функцій послідовності є псевдовипадковими (є ризик повторення набору послідовності);
- ключ необхідно зберігати в базі даних до моменту дешифрування повідомлення, що недопустимо у разі, якщо зловмисники заволодіють базою даних;
- довжина ключа повинна співпадати з довжиною повідомлення, що означає двохкратне збільшення необхідного для зберігання повідомлення об'єму пам'яті. Також це накладає обмеження на пропускну можливість передачі даних.

Вирішення проблеми

Для вирішення проблеми з повторенням послідовності чисел та для забезпечення можливості передачі повідомлення в режимі реального часу можна використовувати алгоритмічні функції генерації псевдовипадкових чисел з додатковими засобами перетворення даних, а саме:

- використання хеш-функцій [3];
- використання додаткових даних [3];

При цьому хеш-функції повинні відповідати сучасним вимогам безпеки (наприклад, серед хеш-функцій сімейства SHA можна застосовувати SHA-512) та не використовуватися в чистому вигляді, при можливості необхідно застосовувати декілька різних хеш-функцій в алгоритмічно визначеному порядку або використовувати такі хеш-функції, які дозволяють налаштовувати силу хешування (Blowfish) [4].

Додаткові дані повинні бути однаковими в одному циклі шифрування-дешифрування, тому не можна застосовувати дані, які можуть змінюватися (системні дата та час, IP-адреса). Також додаткові дані не повинні бути часто вживаними (односимвольні строки). У якості додаткових даних можна використовувати наперед визначені символьні строки випадкових даних.

При цьому, застосування в алгоритмі шифрування-дешифрування різних засобів перетворення даних дасть можливість максимально наблизити отриману послідовність символів (ключа) до повної рівномірної випадковості.

Для вирішення проблеми необхідності зберігання ключа з виключенням можливості несанкціонованого доступу до нього можна використати підхід зберігання початкової послідовності символів, до якої для дешифрування будуть застосовуватись вищеописані додаткові засоби перетворення даних. Проблему виключення можливості ідентифікації зловмисником початкової послідовності символів генерації ключа можна вирішити, якщо записувати ключ в одне поле разом з зашифрованим повідомленням, причому положення символів ключа серед символів повідомлення за один цикл шифрування-дешифрування має бути сталим.

Витрати на зберігання даних можна контролювати зменшенням довжини початкової послідовності символів для генерації ключа по відношенню до довжини повідомлення з наступною генерацією остаточного ключа. Алгоритм генерування ключа включатиме в себе функцію збільшення довжини ключа на базі функцій перетворення даних, які, в свою чергу, включатимуть у себе застосування таких додаткових даних, що не можуть змінитися за один цикл шифрування-дешифрування та водночас змінюються при кожному збільшенні довжини ключа.

Для уникнення можливості несанкціонованого перехвату конфіденційних даних сайт, на якому використовується будь-яка система шифрування-дешифрування даних, повинен бути оснащений технологією шифрування з'єднання HTTPS.

Висновки

Таким чином, вищеописаний підхід до найбільш точного застосування принципів шифрування Вернама з урахуванням типових проблем зберігання та передачі даних на веб-сайтах з використанням систем управління базами даних дозволяє:

- уникнути несанкціонованого дешифрування конфіденційних даних у разі заволодіння базою даних зловмисниками;
- зменшити затрати на зберігання та передачу ключа шифрування-дешифрування.

REFERENCES

1. Шифр Вернама [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Шифр_Вернама
2. Шифрування Вернама [Електронний ресурс] – Режим доступу: http://cryptowiki.net/index.php?title=Шифр_Вернама
3. Криптография и главные способы шифрования данных [Електронний ресурс] – Режим доступу: https://proglib.io/p/methods-of-encryption/
4. Криптографічні хеш-функції [Електронний ресурс] – Режим доступу: http://cryptowiki.net/index.php?title=Криптографические_хэш-функции

Савчук Тамара Олександрівна – PhD, професор, професор кафедри комп'ютерних наук ВНТУ, Вінницький національний технічний університет, м. Вінниця, e-mail:savchtam@gmail.com

Чернобай Олексій Олексійович — студент факультету інформаційних технологій та комп’ютерної інженерії, кафедри комп'ютерних наук ВНТУ, Вінницький національний технічний університет, м. Вінниця, e-mail: alechb19021994@gmail.com

Tamara O. Savchuk – PhD, Professor, Professor of the Computer Sciences Chair, Vinnytsia National Technical University, Vinnytsia, e-mail:savchtam@gmail.com

Olexii O. Chernobai — student of Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : alechb19021994@gmail.com