УДК 004.056.55

Я. Ю. Яремчук

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ПІДВИЩЕННЯ СТІЙКОСТІ ПРОТОКОЛУ АУТЕНТИФІКАЦІЇ WPA-PSK

Вінницький національний технічний університет

Анотація

В роботі розглянуто та детально проаналізовано процес роботи протоколу аутентифікації WPA-PSK, а також описано основний його недолік. Крім того запропоновано модифікацію для процесу генерації ключа підтвердження за рахунок використання додаткової операції вживлення порції випадкового числа, що генерується всередині PMK. Отримана криптостійкість ключа підтвердження є вищою за оригінальну майже на 28%.

Ключові слова: WPA-PSK, протокол аутентифікації, криптографія, криптостійкість.

Abstract

The paper examines and analyzes the process of the WPA-PSK authentication protocol, as well as describes its main disadvantage. In addition, a modification is proposed for the process of generating a confirmation key by using an additional operation of feeding a portion of a random number generated within the PMK. The received cryptostability of the confirmation key is higher than the original by almost 28%.

Keywords: WPA-PSK, authentication protocol, cryptography, cryptographic stability.

Захист інформації завжди був однією з пріоритетних ланок досліджень в історії людства. Та лише з розвитком інформаційних технологій стало зрозуміло, на скільки дійсно важливим є приватність даних та захищеність каналу їх передачі. Актуальністю захисту інформації в комп'ютерних мережах зокрема є запобігання викрадення чи спотворення інформації, та в цілому – несанкціонованого доступу до неї. На сьогоднішній день більшість електронних гаджетів вимагають підключення до мережі Інтернет через точки доступу WIFI. Найвразливішою ланкою процесу аутентифікації користувача підчас під'єднання до бездротової мережі є частина, що відповідає за обмін секретним ключем між точкою доступу та клієнтом [1].

Ключ доступу до мережі мають як клієнт, так і точка доступу ще до початку процесу з'єднання. Даний ключ, або ж пароль – це секретна інформація що буде використана для того, щоб згенерувати усі необхідні ключі для захисту бездротової мережі. У ході з'єднання генерується декілька ключів для виконання різних задач [2-3]:

1. Спочатку відбувається чотириходове рукостискання - процес з'єднання клієнта та сервера. На його початку клієнт «аутентифікується» та «асоціюється» з точкою доступу. Насправді цей процес не містить ніяких секретних ключів та створений задля обміну системною інформацією між точкою доступу та клієнтом.
2. Далі відбувається процес обміну так званими рукостисканнями. Узгоджений ключ доступу використовується для створення ключа PSK (Pre-shared key).
3. Довжина ключа доступу має довжину від 8 до 63 символів. Використовуючи Password-Based Key Derivation Function 2 (PBKDF2), ключ доступу, назва мережі та кількість символів в її назві хешуються 4096 разів задля створення 256-бітного Pair Master Key (PMK) (рис. 1).

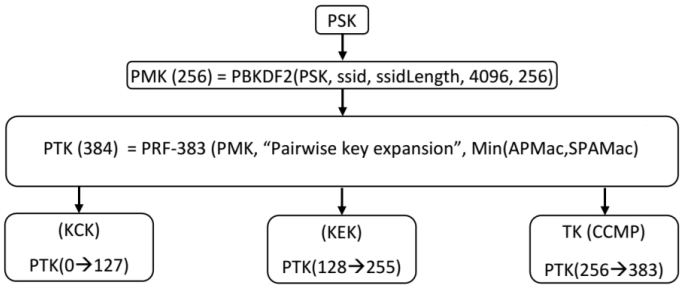

Рисунок 1 – Генерація ключа WPA-PSK

4. Ключ PMK, пароване розширення ключа, MAC-адреси клієнта та точки доступу, випадкові числа що ними генеруються – передаються до псевдовипадкової функції для створення PTK

тимчасового ключа пари. Довжина цього ключа складає 384 біти. Даний ключ містить три підключі, зображені на рисунку 1:

— ключ підтвердження, що використовується для забезпечення цілісності даних в процесі рукостискань;

— ключ шифрування, що потрібен для захисту обміну інформації підчас рукостискань;

— тимчасовий ключ потрібен для захисту даних що передаються в мережі.

Проблемою такого методу аутентифікації та захисту даних являється той факт, що ключ підтвердження перевіряється точкою доступу окремо від всього блоку PSK, а тому завжди існує можливість перехоплення цього блоку зловмисником [4].

Криптостійкість блоку ключа підтвердження визначається за формулою:

$$z = z_h * z_o$$

де z_h - криптостійкість хешованого ключа, z_o - криптостійкість операцій криптоперетворення.

Практична криптостійкість даного ключа визначається наступними параметрами: $M_{mo}(n)$ - кількість матричних операцій вибраної розмірності; n_k – розрядність ключа, M_{on} – кількість операцій у послідовності, яка реалізує команду [5]. Формула практичної криптостійкості має такий вгляд:

$$K_n = (2^{nk} * M_{on}) \log_2 (M_{mo}(n))$$

Дана величина, у свою чергу буде пропорційна величині $z_o = 2^{K_n}$. Враховуючи величину хешу та довжину блоку, отримуємо практичну криптостійкість, що дорівнює $K_n = 32 * \log_2 1456 = 336$, а отже $z_o = 2^{336}$.

Дієвим рішенням по збільшенню криптостійкості ключа підтвердження є використання додаткової операції вживлення порції випадкового числа, що генерується всередині РМК довжиною 8 біт до блоку ключа підтвердження. У даному випадку, додаткова змінна додасть 4 операції до процесу шифрування, тим самим збільшуючи M_{on} на 4 одиниці.

Обчисливши нову криптостійкість ключа $K_n = 48 * \log_2 1456 = 504$, отримали таку криптостійкість операцій криптоперетворення: $z_o = 2^{504}$. Отримана криптостійкість значно перевищує оригінальну на 28%, що є суттєвим покращенням.

Висновки

В ході проведеного дослідження протоколу аутентифікації WPA-PSK було визначено головний його недолік - ключ підтвердження перевіряється точкою доступу окремо від всього блоку PSK, а тому завжди існує можливість перехоплення цього блоку зловмисником. Для вирішення цієї проблеми було запропоновано модифікацію для процесу генерації ключа підтвердження за рахунок використання додаткової операції вживлення порції випадкового числа, що генерується всередині РМК. Отримана криптостійкість ключа підтвердження є вищою за оригінальну на 28%.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Вирішення проблеми доступності до мережі Інтернет шляхом динамічного балансування пропускної здатності каналу WEB-трафіку / Ю.Яремчук, Д. Кец, Т. Жевега, К. Безпалий. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – №1. – С. 58–64.

2. А. В. Соколов. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. - ДМК Пресс., 2012. – 656с.

3. Hacker Dictionary [Electronic Resource]. – Mode of access : URL : http://www.robergraham.com/hacker-dictionary. - Назва з екрану.

4. Coron, J.-S., Naccache, D., Tibouchi, M.: Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers. In: Pointcheval, D., Johansson, T. (eds.) CA, 2011.

5. Huang, Y., Evans, D., Katz, J., Malka, L.: Faster secure two-party computation using garbled circuits., 2010.

Яремчук Яна Юріївна — студент, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: yanunova@hotmail.com.

Науковий керівник: ***Карпінець Василь Васильович*** — кандидат технічних наук, доцент, завідувач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця.

Yaremchuk Yana Yuriivna — student, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnytsia, e-mail: yanunova@hotmail.com.

Supervisor: ***Karpinets Vasyl V.*** — Ph. D., assistant professor, Head of the Department of Management and Security of Information Systems, Vinnitsa National Technical University, Vinnytsia.