УДК 621.391.8

Д. В. Михалевський
І. А. Самолюк

ДОСЛІДЖЕННЯ МЕТОДУ ШИФРУВАННЯ ДАНИХ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ WPA3

Вінницький національний технічний університет

Анотація
В роботі проведено дослідження методу шифрування стандарту 802.11 підключень за допомогою технології WPA3.
Ключові слова: WPA, Wi-Fi, шифрування даних, бездротова мережа стандарту 802.11

Abstract
The work investigates method of encryption of 802.11 standart by using WPA3 technology.
Keywords: WPA, Wi-Fi, data encryption, 802.11 wireless network.

Вступ

Для створення ключа безпеки бездротової мережі 802.11 користувачеві необхідно придумати унікальний код, який буде відкривати або закривати доступ до його особистої мережі. В цьому випадку головним є не сам ключ, а тип шифрування інформації, що протікає між роутером і ПК. Дана процедура створена для підвищення безпеки переданої інформації і передбачає, що якщо введений неправильний ключ, то пристрій не зможе її розкодувати.

На сьогоднішній день існують наступні типи шифрування Wi-Fi підключень [1]:

1. WPA (Wi-Fi Protected Access)**;**
2. WPA2 (Wi-Fi Protected Access II);
3. WEP (Wired Equivalent Privacy).
4. WPA3 (Wi-Fi Protected Access III);

У даній статті буде розглядатися тип шифрування Wi-Fi підключень за допомогою технології WPA3 **(**Wi-Fi Protected Access III**)**.

Основна частина

WPA – це специфікація шифрування даних для бездротової мережі, що є стандартом безпеки 802.11 [1]. У 2017 році в стандарті WPA2 була виявлена серйозна уразливість, що отримала назву KRACK (Key Reinstallation Attack) - атака з перевстановлення ключа. Цей факт, поряд з усіма раніше відомими недоліками WPA2, підштовхнув Wi-Fi Alliance до розробки нового стандарту безпеки - WPA3 [2].

Стандарт 802.11 вже давно став невід'ємною частиною життя мільйонів людей, а з появою IoT число бездротових пристроїв у всьому світі постійно зростає [1], тому питання захисту 802.11 мереж не втрачають своєї актуальності. Попередня версія WPA2 була введена в 2004 році і за останні кілька років неодноразово була дискредитована [3].

У WPA3 за аналогією з WPA2 залишається два режими роботи: WPA3-Enterprise і WPA3-Personal.

WPA3-Personal відрізняється більш простим вибором пароля, щоб користувачі могли легко запам'ятати його. Він також володіє більш високим рівнем безпеки, при якому збережені дані і трафік даних в мережі не будуть скомпрометовані, навіть якщо пароль зламаний і дані вже були передані. Оновлення також дозволило здійснити одночасну аутентифікацію Equals (SAE), яка замінила Pre-shared Keys (PSK) в WPA2-Personal [4].

WPA3-Enterprise був побудований в основному для більш жорсткого і послідовного застосування протоколів безпеки в мережах урядів, установ, підприємств і фінансових установ. Пропонуючи додаткову 192-розрядну мінімальну захист, WPA3 зробить криптографічні інструменти краще. Отже, більш надійний захист конфіденційних даних [5].

Головними відмінностями WPA3 є наступні особливості:

— *Швидке підключення пристроїв Wi-Fi.* Як вже говорилося, просте з'єднання краще в WPA3 і те, чого не вистачає в технології WPA2. Додавання пристроїв IoT, таких як динаміки WiFi і WiFi камери, може бути як небезпечним, так і складним. Це пов'язано з тим, що ці пристрої не дозволяють користувачеві вводити паролі і налаштовувати параметри безпеки. Для цього потрібно стороння програма або додаток, що робить ці пристрої уразливими для атак і кіберзлочинців. Підвищена безпека домашніх пристроїв за допомогою QR-кодів також є однією з функцій, яку WPA3 пропонує і недоступною для WPA2 [6].

— *Підвищена безпека мереж загального користування.* Якщо використовуються точки доступу WiFi в громадських місцях - це, як правило, ризиковане заняття. Вона схильна до атак, так як є відкритою і незахищеною мережею. WPA3, в свою чергу, забезпечує більш високу безпеку даних при підключенні до нього. Це означає, що дані, що відправляються і одержуються по незахищеній мережі, залишатимуться зашифрованими і безпечними. Це працює, навіть якщо в мережі немає пароля для захисту.

— *Підвищена безпека підприємства.* WPA3, на відміну від WPA2, надає 192-бітний пакет безпеки, який забезпечує більш надійну систему безпеки для корпоративних середовищ. Більші ключі шифрування використовуються особливо на важливих підприємствах, таких як оборона, промислові підприємства і, звичайно ж, уряд. Чим більше розмір ключа, тим вища безпека шифрування даних. Це також ускладнює проникнення хакерів в критично важливі мережі [7].

— *Протокол надання пристрою WiFi.* Замість загальних паролів, WPA3 зможе реєструвати нові пристрої, які не зажадають цього в процесі. Нова система називається «Протокол надання Wi-Fi-пристроїв» (Wi-Fi DPP). Система функціонує шляхом передачі процедури отримання доступу по повітрю без передачі пароля. QR-коди і мітки NFC використовуються користувачами для підключення до мережі. Пристрій можна аутентифікувати по мережі, зробивши фотографію або прийнявши радіосигнал від маршрутизатора [7].

Висновки

Таким чином, стрибок в цифрову епоху в значній мірі пов'язаний з розвитком Інтернету і технологій бездротових мереж. Бездротові мережі постійно вдосконалюють свої послуги, підвищуючи безпеку і продуктивність.

А проведені вище дослідження підтвердили те що, технологія WPA3 достатньо надійна і забезпечує високий рівень захищеності бездротових мереж. Це черговий прорив на шляху до посилення безпеки бездротових з'єднань, але потрібно буде декілька років, щоб повністю реалізувати WPA3 в деяких країнах світу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Mykhalevskiy, D. (2018). Construction of mathematical models for the estimation of signal strength at the imput to the 802.11 standard receiver in a 5 GHz band. Eastern-European Journal of Enterprise Technologies, 6/9(96), 16-21. DOI: 10.15587/1729-4061.2018.150983.

2. Lashkari, A.H.; Danesh, M.M.S.; Samadi, B. A survey on wireless security protocols (WEP, WPA andWPA2/802.11). In Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology, Beijing, China, 8–11 August 2009; pp. 48–49.

3. Mykhalevskiy D. Development of a mathematical model for estimating signal strength at the input of the 802.11 standard receiver / D. Mykhalevskiy, N. Vasylkivskiy, O. Horodetska – Easten-European Journal of Enterprise Technologies. 2017. №4/9 (88). Pp. 38-43. DOI: 10.15587/1729-4061.2017.114191.

4. Михалевський Д. В. Дослідження передачі інформації в умовах суміщеного та сусіднього інтерференційного каналів для стандарту 802.11n / Д. В. Михалевський, В.В. Номировська, О.М. Постернак // Вимірювальна та обчислювальна техніка в технологічних процесах.– 2015. – №2. – С. 152 – 153.

5. Михалевський Д. В. Оцінка ефективної швидкості передачі інформації для сімейства стандартів 802.11x у діапазоні 2.4 ГГц / Д. В. Михалевський, О. С. Городецька. – Сборник научных трудов Sword. – Выпуск 3(40). Том 3. Иваново: Научный мир, 2015. – С.43-44.

6. Vanhoef, M.; Piessens, F. Key reinstallation attacks: Forcing nonce reuse in WPA2. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October – 3 November 2017; pp. 1313–1316.

7. Ahmad, M.S.; Tadakamadla, S. Short paper: Security evaluation of IEEE 802.11 w specification. In Proceedings of the fourth ACM conference on Wireless network security, Hamburg, Germany, 14 – 17 June 2011; pp. 53–55.

Михалевський Дмитро Валерійович — канд. техн. наук, доцент кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університет.

Самолюк Ірина Анатоліївна — студентка групи ІТТ-19м, факультет інфокомунікацій радіоелектроніки та наносистем, Вінницький національний технічний університет, м. Вінниця.

Mikhalevskiy Dmytro — Cand. Sc. (Eng), Associate Professor at the Department of Telecommunication System and Television, Vinnytsia National Technical University, Vinnytsia.

Samoliuk Iryna — Department of Infocommunication, Electronics and Nanosystems, Vinnytsia National Technical University, Vinnytsia.