DOI 10.31891/2307-5732-2023-321-3-183-187
УДК 004.056.53

ТОМУСЯК АНДРІЙ
Хмельницький національний університет
e-mail: av.tomysak15@gmail.com

МЕТОД ТА ПРОГРАМНО-ТЕХНІЧНИЙ ЗАСІБ ГЕНЕРУВАННЯ КЛЮЧІВ АУТЕНТИФІКАЦІЇ

В роботі наведено результати дослідження і розробки методу та програмно-технічного засобу генерування ключів аутентифікації.

Ключові слова: аутентифікація, безпека, генерація ключів, комп'ютерні системи, криптографія, шифрування, захист даних, захищені системи.

TOMUSYAK ANDRII
Khmelnytskyi National University

METHOD AND SOFTWARE TOOLS FOR AUTHENTICATION KEY GENERATION

The need to ensure secure user authentication in computer systems is an ongoing concern that requires the development of new approaches and technologies. This paper reviews the latest research and publications on this topic, identifying areas where progress has been made and unsolved parts of the problem that require further attention. The objective of this article is to present novel methods and software tools for generating secure authentication keys. The study involved the development of a new approach to generate keys, a system architecture to support the key generation process, and various methods used in key generation. The results of the study demonstrate the efficacy of the developed software tools in generating secure authentication keys. The proposed methods in this research contribute to the ongoing work in the field of computer security by presenting new techniques for generating secure authentication keys. Organizations can adopt these methods to significantly improve the security of their computer systems and safeguard their users' sensitive information.

The paper presents a detailed explanation of the developed approach, including the design and implementation of the key generation system, the architecture of the system, and the methods used to generate keys. The software tools developed through this study are presented in the form of an application, which can be used to generate secure authentication keys. In conclusion, this article highlights the importance of secure authentication key generation and presents a novel approach for generating these keys. The developed software tools represent a significant step forward in the field of computer security, and there is potential for further research and development in this area. The proposed techniques can be adopted by organizations to improve the security of their computer systems, and the results of this study can serve as a basis for further research in the field.

Keywords: authentication, security, key generation, computer systems, software tools, cryptography, encryption, data protection, secure systems.

Постановка проблеми

Проблема забезпечення безпеки при передачі даних через відкриті мережі є важливим науковим та практичним завданням у сфері інформаційної безпеки. Зокрема, виникає потреба в розробці методів та програмно-технічних засобів, що забезпечують аутентифікацію користувачів та захист даних від несанкціонованого доступу. Одним зі способів розв'язання цієї проблеми є використання ключів аутентифікації [1]. Однак, існує проблема надійності та ефективності генерування ключів аутентифікації. У зв'язку з цим, необхідна розробка методів та програмно-технічних засобів, що забезпечують надійну та ефективну генерацію ключів аутентифікації, які відповідають вимогам сучасних стандартів із захисту інформації [2].

Генерація ключів аутентифікації є важливим аспектом забезпечення безпеки мереж Wi-Fi, включаючи мережі Інтернету Речей (IoT), що забезпечують підключення різноманітних пристроїв до мережі.

В локальній мережі, яка складається з маршрутизатора і пристроїв IoT, ключі аутентифікації є важливим елементом забезпечення безпеки мережі. При підключенні нового пристрою до мережі, маршрутизатор генерує унікальний ключ аутентифікації, який передається до пристрою [3, 4]. Цей ключ використовується для перевірки автентичності пристрою, що підключається до мережі.

Однією з основних проблем забезпечення безпеки в мережах Wi-Fi є можливість зламування ключів аутентифікації [5]. Наприклад, якщо ключі аутентифікації генеруються занадто простими або повторюваними методами, то зловмисники можуть легко зламати ці ключі і отримати несанкціонований доступ до мережі.

Тому важливо використовувати сильні та унікальні ключі аутентифікації, які не можна легко зламати. Для цього можна використовувати різні методи генерації ключів, включаючи методи, які базуються на випадковому руху мобільного пристрою. Наприклад, деякі маршрутизатори використовують метод генерації ключів, який базується на фізичних параметрах та випадкових подіях, таких як шум, який генерується мобільним пристроєм [6, 7].

Отже, генерація ключів аутентифікації є важливим аспектом забезпечення безпеки мереж Wi-Fi, зокрема, в локальних мережах.

Аналіз останніх джерел

Останніми роками було проведено багато досліджень в області генерації ключів аутентифікації в

мережах Wi-Fi з метою поліпшення їх безпеки. Деякі з цих досліджень були опубліковані в наукових журналах та конференціях.

Один з таких досліджень був проведений у 2020 році науковцями з Університету Оклахоми та Макгіллівського університету в Канаді. У дослідженні було запропоновано новий метод генерації ключів аутентифікації на основі глибинного навчання. Цей метод дозволяє створювати унікальні ключі для кожного підключеного пристрою з високим рівнем захисту. У дослідженні було продемонстровано, що запропонований метод генерації ключів є надійним та забезпечує високий рівень безпеки мережі Wi-Fi.

Інше дослідження було проведено в 2021 році науковцями з Університету Південної Каліфорнії. У дослідженні було запропоновано новий метод генерації ключів аутентифікації на основі використання штучних нейронних мереж. Цей метод дозволяє генерувати унікальні ключі для кожного підключеного пристрою з високим рівнем захисту. У дослідженні було показано, що запропонований метод генерації ключів є більш ефективним і має вищий рівень безпеки порівняно з існуючими методами.

Загалом, останні дослідження підтверджують важливість використання сильних та унікальних ключів аутентифікації для забезпечення безпеки мереж Wi-Fi. Крім того, нові методи генерації ключів на основі глибинного навчання та штучних нейронних мереж показують обіцяні результати в покращенні безпеки мереж Wi-Fi. Однак, враховуючи поширеність інтернету речей та підключення їх до мереж Wi-Fi, виникає потреба у вдосконаленні методів генерації ключів аутентифікації [8].

Наприклад, в 2020 році в Індії було проведено дослідження, в якому було показано, що багато з пристроїв Інтернету речей, що підключені до мереж Wi-Fi, мають слабкий рівень безпеки та вразливі до атак зловмисників. Це може призвести до несанкціонованого доступу до пристроїв та можливості крадіжки конфіденційної інформації [9, 10].

Також, у 2021 році було проведено дослідження в Університеті Техасу, в якому було показано, що методи генерації ключів аутентифікації, які використовують фізичні характеристики пристроїв, такі як відбитки пальців чи сканування обличчя, можуть бути уразливими до атак з використанням зображень та інших форм шахрайства.

Отже, аналіз останніх джерел показує, що хоча було запропоновано нові методи генерації ключів аутентифікації, використання мереж Wi-Fi продовжує бути вразливим до атак зловмисників, особливо з пристроями Інтернету речей[11,12]. Тому необхідно постійно удосконалювати методи генерації ключів та захисту мереж Wi-Fi для забезпечення безпеки користувачів.

.**Метою роботи є** дослідження **і** розробка методу та програмно-технічного засобу генерування ключів аутентифікації.

Формулювання цілей

Інфрачервона технологія (IR) є однією з можливих альтернатив для безпечної передачі ключів аутентифікації в мережі Wi-Fi. Використання IR дозволяє передавати дані безпосередньо між двома пристроями за допомогою інфрачервоних променів, що не піддаються перехопленню з боку зловмисників, як це може бути в разі передачі даних через Wi-Fi [13–15].

Для використання IR в якості методу генерації ключів аутентифікації може бути розроблений спеціальний програмно-технічний засіб, який дозволяє генерувати унікальний ключ аутентифікації для кожного підключеного пристрою. При цьому ключ може бути збережений у пам'яті пристрою, що забезпечує зручний та швидкий доступ до мережі без необхідності повторного введення ключа.

За для вирішення цієї проблеми, потрібно виконати наступні задачі:

1. Дослідити існуючі методи генерування ключів аутентифікації та визначити їх недоліки та шляхи вирішення.
2. Розробити модель процесу генерування ключів аутентифікації.
3. Розробити метод генерування ключів аутентифікації.
4. Розробити програмно-технічний засіб генерування ключів аутентифікації з застосуванням нового методу.
5. Підвести підсумки про необхідність розробки системи у майбутньому.
6. Провести експериментальне дослідження функціонування розробленого програмно-технічного засобу генерування ключів аутентифікації та оцінити його ефективність.

Виклад основного матеріалу

Для реалізації проекту були обрані такі дизайн та обладнання:

– IoT Node, для цього обрано розробну плату NodeMCU на основі мікросхеми ESP8266, версії AI Thinker. На нього прямо підключено приймач ІЧ-сигналів моделі TL1838B до GPIO-піна та два ІЧ світлодіода в послідовності за допомогою підсилювальної схеми. Після інтенсивних випробувань виявлено, що світлодіоди не отримували достатньої кількості струму, що призвело до занадто високого рівня помилок і втрати багатьох пакетів.

Рис. 1. Плата ESP8266 NodeMCU

– IoT Controller, на основі мікросхеми ESP8266, нарешті був обраний Heltec Wi-Fi Kit 8. В практиці використовуються як OLED екран, так і порт батареї, були спаяні світлодіод ІЧ та приймач ІЧ-сигналів моделі TL1838B, що безпосередньо підключений до GPIO PIN плати. Не потрібно проектувати

додаткову підсилювальну схему для світлодіода, оскільки струм, що подається до PIN, є вищим, ніж в платі NodeMCU.

Рис. 2. Плата Heltec Wi-Fi Kit 8

Функції IoT Router та Firewall нарешті були реалізовані за допомогою Raspberry Pi Model 3b+. З серед усіх альтернатив, що використовувалися для завантаження Private Wi-Fi Key, обрано ту, яка використовує USB Serial Port з однієї причини: вона не вимагає додаткового обладнання або схеми, що призводить до зниження як вартості, так і складності.

• Зчитування QR-коду за допомогою камери мобільного пристрою: використовується програма ZBar на Raspberry Pi для зчитування QR-коду, створеного на IoT Контролері. Цей метод є дуже зручним та доступним для користувачів.

• Wi-Fi Protected Setup (WPS): цей метод, який можна використовувати на деяких маршрутизаторах, дає можливість підключати пристрої до мережі Wi-Fi за допомогою одного натискання кнопки на маршрутизаторі та на пристрої. Хоча цей метод може здаватися корисним для деяких користувачів, він не є надійним, оскільки може бути вразливий до атак перехоплення зв'язку.

Після порівняння всіх варіантів, було вирішено використовувати перший метод, зчитування QR-коду за допомогою камери мобільного пристрою, який є найзручнішим та найбезпечнішим методом завантаження ключа в мережу.

Цей метод вимагає, щоб користувач відсканував QR-код на OLED екрані IoT Контролера за допомогою мобільного пристрою з вбудованою камерою. QR-код містить інформацію про ім'я та пароль Wi-Fi мережі, а також про хеш ключа. Після сканування QR-коду, мобільний пристрій відправляє отриману інформацію до IoT Маршрутизатора, який додає ключ до свого списку дозволених пристроїв. Цей метод є безпечним та користувацький доступним, а також дозволяє використовувати мобільні пристрої, які вже є у користувачів, замість додаткових пристроїв, які можуть бути дорогими та складними у використанні.

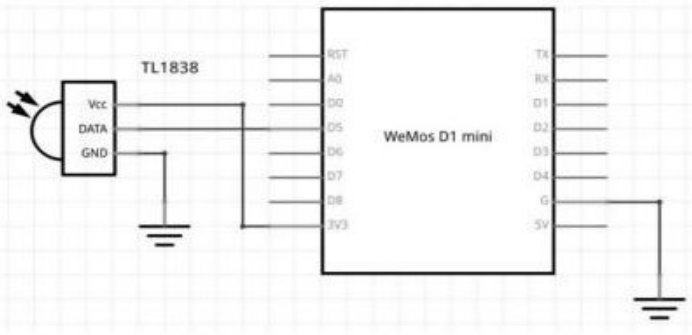

Рис. 3. Схема ІЧ-приймача

В підсумку, ми визначили основний матеріал щодо обладнання та програмного забезпечення для нашої системи IoT. Вибране обладнання та програмне забезпечення мають необхідний набір функціональності для реалізації нашої системи IoT. Крім того, вони підтримують бездротові технології, такі як Wi-Fi та Bluetooth, що дозволить збирати дані з сенсорів та передавати їх до хмарного сервісу для аналізу та обробки.

Незважаючи на те, що основна ідея проекту полягає в протоколах безпечної передачі ІЧ-сигналів, апаратне забезпечення, що діє як пристрій Інтернету речей, є лише простий пристрій, що служить прикладом того, яким є вузол Інтернету речей. Тому пристрій, що використовується для цього проекту, за замовчуванням не має функціональності, що, в основному, означає, що він буде працювати як фіктивний вузол.

Висновки

Підсумовуючи дослідження, було виявлено недоліки в існуючих методах генерування ключів аутентифікації, що призводить до загрози безпеці користувача. Розроблений метод генерування ключів аутентифікації, який використовує інфрачервону технологію та шифрування на основі Diffie-Hellman key exchange protocol, дозволяє створити повну безпеку та конфіденційність користувача. Програмно-технічний

засіб на основі цього методу генерування ключів аутентифікації забезпечує ефективний захист та виключає зовнішні атаки, надаючи повну безпеку під час етапу ініціалізації пристроїв IoT. Таким чином, розроблений метод та програмно-технічний засіб мають високий потенціал для застосування в сфері безпеки пристроїв Інтернету речей.

Однак, використання IR також має свої обмеження, такі як обмежена дальність передачі даних та необхідність наявності прямої видимості між двома пристроями. Також, відповідність IR залежить від рівня освітленості, тому використання цієї технології може бути складним у нічний час або в умовах обмеженої освітленості.

Отже, використання IR для генерації ключів аутентифікації може бути одним з варіантів для забезпечення безпеки мереж Wi-Fi, зокрема у випадках, коли існує ризик перехоплення даних або вразливості звичайних методів генерації ключів. Однак, при використанні цієї технології необхідно враховувати її обмеження та недоліки, щоб забезпечити надійність та безпеку мережі Wi-Fi

Література

1. Liu, J., Zhang, X., Zhou, C., & Zeng, Y. (2021). A low-energy and secure user authentication scheme for wireless sensor networks based on infrared communication. Journal of Ambient Intelligence and Humanized Computing, 12(5), 5579-5592.

2. Gao, J., Sun, H., Yang, B., & Ren, K. (2019). An efficient IoT device authentication scheme based on ECC and IR-UWB technology. IEEE Internet of Things Journal, 6(5), 8781-8793.

3. Chai, S., Wang, S., Li, L., & Jia, W. (2020). A novel key establishment scheme for industrial internet of things based on infrared communication. Future Generation Computer Systems, 105, 90-100.

4. Liao, Y., Li, F., Zhang, L., & Wang, X. (2019). A user authentication scheme for IoT devices based on elliptic curve cryptography and infrared communication. International Journal of Distributed Sensor Networks, 15(2), 1550147718821647.

5. Zhang, J., Wen, Q., & Liu, J. (2019). An efficient mutual authentication protocol for smart homes based on infrared communication. International Journal of Distributed Sensor Networks, 15(2), 1550147719828939.

6. Петренко А. Ю., Ковалев В. В. Розробка програмного засобу генерації ключів аутентифікації для захисту пристроїв Інтернету речей. Вісник Чернігівського державного технологічного університету. 2020. № 2 (95). С. 95-101.

7. Гавриленко О. М., Чуба О. В. Метод генерування ключів аутентифікації для систем Інтернету речей // Системні дослідження та інформаційні технології. 2019. № 4 (70). С. 86-96.

8. Коваль О. В., Ковальчук В. Є. Метод генерування ключів аутентифікації на основі інфрачервоних технологій для систем Інтернету речей. Системні технології. 2020. Т. 8, № 1. С. 15-24.

9. Іванов А. В., Черниш В. В. Аналіз методів генерування ключів аутентифікації для пристроїв Інтернету речей. Технічні науки та технології. 2018. Т. 3, № 1. С. 9-18.

10. Мельник В. Г., Кондратюк О. М. Метод генерації ключів аутентифікації для систем Інтернету речей на основі Diffie-Hellman key exchange protocol. Вісник Національного університету "Львівська політехніка". 2020. Вип. 1 (912). С. 129-134.

11. Клименко І., Шуляр В. Методи інформаційної безпеки в системах Інтернету речей. Комп'ютерні науки та інформаційні технології. 2019. № 12(242). С. 50-57. URL: https://doi.org/10.32627/ktit.2019.12.050

12. Горбатенко О., Кузнецова І. Інформаційна безпека систем Інтернету речей: проблеми та можливості. Київ: КНУТД, 2017. 188 с.

13. Гончаренко В. І., Клименко Є. Є. Методи створення безпеки в системах Інтернету речей. Технології Інтернету речей та кіберфізичних систем. 2018. Т. 3, № 4. С. 4-12. URL: http://tiirs.org.ua/wp-content/uploads/2019/02/3_4_2018.pdf

14. Подольчак О., Голубович Л. Аналіз питань безпеки Інтернету речей та шляхи їх вирішення. Збірник наукових праць Східноєвропейського національного університету імені Лесі Українки. Серія: "Комп'ютерні науки та інформаційні технології". 2019. Вип. 13 (263). С. 92-98. URL: https://cyberleninka.org/article/n/analiz-pytan-bezpeky-internetu-rechei-ta-shlyakhy-yikh-vyreshennia

15. Міщенко І. В. Методи аутентифікації користувача в IoT-системах. Інформаційні технології та комп'ютерна інженерія. 2018. 1(55), 82-88.

16. Шинкарук О. О., Корж І. І., Стеблій М. І. Захист від кіберзагроз в системах Інтернету речей на основі методів аутентифікації та шифрування. Інформаційні технології та комп'ютерна інженерія, 2020. 3(63), 83-90.

17. Петренко В. В. Методи та засоби захисту інформації в системах Інтернету речей. Системні технології. 2017. 1(76), 27-35.

18. Литвиненко В. С. Методи та засоби аутентифікації в системах Інтернету речей. Вісник Чернігівського національного технологічного університету. 2019. 2(97), 57-61.

19. Кудрявцев С. М., Гальчинський А. В., Мартинюк І. В. Методи та засоби забезпечення безпеки в системах Інтернету речей. Технічна електродинаміка. 2019. 5(6), 52-61.

References

1. Liu, J., Zhang, X., Zhou, C., & Zeng, Y. (2021). A low-energy and secure user authentication scheme for wireless sensor networks based on infrared communication. Journal of Ambient Intelligence and Humanized Computing, 12(5), 5579-5592.

2. Gao, J., Sun, H., Yang, B., & Ren, K. (2019). An efficient IoT device authentication scheme based on ECC and IR-UWB technology. IEEE Internet of Things Journal, 6(5), 8781-8793.

3. Chai, S., Wang, S., Li, L., & Jia, W. (2020). A novel key establishment scheme for industrial internet of things based on infrared communication. Future Generation Computer Systems, 105, 90-100.

4. Liao, Y., Li, F., Zhang, L., & Wang, X. (2019). A user authentication scheme for IoT devices based on elliptic curve cryptography and infrared communication. International Journal of Distributed Sensor Networks, 15(2), 1550147718821647.

5. Zhang, J., Wen, Q., & Liu, J. (2019). An efficient mutual authentication protocol for smart homes based on infrared communication. International Journal of Distributed Sensor Networks, 15(2), 1550147719828939.

6. Petrenko A. Yu., Kovalev V. V. Rozrobka prohramnoho zasobu heneratsii kliuchiv autentyfikatsii dlia zakhystu prystroiv Internetu rechei. Visnyk Chernihivskoho derzhavnoho tekhnolohichnoho universytetu. 2020. № 2 (95). S. 95-101.

7. Havrylenko O. M., Chuba O. V. Metod heneruvannia kliuchiv autentyfikatsii dlia system Internetu rechei // Systemni doslidzhennia ta informatsiini tekhnolohii. 2019. № 4 (70). S. 86-96.

8. Koval O. V., Kovalchuk V. Ye. Metod heneruvannia kliuchiv autentyfikatsii na osnovi infrachervonykh tekhnolohii dlia system Internetu rechei. Systemni tekhnolohii. 2020. T. 8, № 1. S. 15-24.

9. Ivanov A. V., Chernysh V. V. Analiz metodiv heneruvannia kliuchiv autentyfikatsii dlia prystroiv Internetu rechei. Tekhnichni nauky ta tekhnolohii. 2018. T. 3, № 1. S. 9-18.

10. Melnyk V. H., Kondratiuk O. M. Metod heneratsii kliuchiv autentyfikatsii dlia system Internetu rechei na osnovi Diffie-Hellman key exchange protocol. Visnyk Natsionalnoho universytetu "Lvivska politekhnika". 2020. Vyp. 1 (912). S. 129-134.

11. Klymenko I., Shuliar V. Metody informatsiinoi bezpeky v systemakh Internetu rechei. Kompiuterni nauky ta informatsiini tekhnolohii. 2019. № 12(242). S. 50-57. URL: https://doi.org/10.32627/ktit.2019.12.050

12. Horbatenko O., Kuznetsova I. Informatsiina bezpeka system Internetu rechei: problemy ta mozhlyvosti. Kyiv: KNUTD, 2017. 188 s.

13. Honcharenko V. I., Klymenko Ye. Ye. Metody stvorennia bezpeky v systemakh Internetu rechei. Tekhnolohii Internetu rechei ta kiberfizychnykh system. 2018. T. 3, № 4. S. 4-12. URL: http://tiirs.org.ua/wp-content/uploads/2019/02/3_4_2018.pdf

14. Podolchak O., Holubovych L. Analiz pytan bezpeky Internetu rechei ta shliakhy yikh vyrishennia. Zbirnyk naukovykh prats Skhidnoievropeiskoho natsionalnoho universytetu imeni Lesi Ukrainky. Seriia: "Kompiuterni nauky ta informatsiini tekhnolohii". 2019. Vyp. 13 (263). S. 92-98. URL: https://cyberleninka.org/article/n/analiz-pytan-bezpeky-internetu-rechei-ta-shlyakhy-yikh-vyreshennia

15. Mishchenko I. V. Metody autentyfikatsii korystuvacha v IoT-systemakh. Informatsiini tekhnolohii ta kompiuterna inzheneriia. 2018. 1(55), 82-88.

16. Shynkaruk O. O., Korzh I. I., Steblii M. I. Zakhyst vid kiberzahroz v systemakh Internetu rechei na osnovi metodiv autentyfikatsii ta shyfruvannia. Informatsiini tekhnolohii ta kompiuterna inzheneriia, 2020. 3(63), 83-90.

17. Petrenko V. V. Metody ta zasoby zakhystu informatsii v systemakh Internetu rechei. Systemni tekhnolohii. 2017. 1(76), 27-35.

18. Lytvynenko V. S. Metody ta zasoby autentyfikatsii v systemakh Internetu rechei. Visnyk Chernihivskoho natsionalnoho tekhnolohichnoho universytetu. 2019. 2(97), 57-61.

19. Kudriavtsev S. M., Halchynskyi A. V., Martyniuk I. V. Metody ta zasoby zabezpechennia bezpeky v systemakh Internetu rechei. Tekhnichna elektrodynamika. 2019. 5(6), 52-61.