УДК 681.12

М. Д. Кренцін
Л. М. Куперштейн

ВИКОРИСТАННЯ NFC ДЛЯ ЗАХИЩЕНОГО ОБМІНУ ІДЕНТИФІКАЦІЙНИМИ ДАНИМИ У ПІРИНГОВИХ МЕРЕЖАХ

Вінницький національний технічний університет

Анотація

Запропоновано метод захищеного обміну ідентифікаційними даними у пірингових мережах. Метод базується на комбінованому використанні технології NFC та методі доказу з нульовим знанням. Розроблений метод забезпечує конфіденційність, відмовостійкість, захист від атак з перехопленням трафіку, надійність верифікації та захист від несанкціонованого доступу.

Ключові слова: пірингова мережа, доказ нульового знання, NFC, комунікація, шифрування, GUID.

Abstract

A method of a secure method of exchanging identification data in peering networks is proposed. The method is based on the combined use of NFC technology and the zero-knowledge proof method. The developed method ensures communication security, confidentiality, fault tolerance, protection against traffic interception attacks, verification reliability and protection against unauthorized access.

Keywords: peer-to-peer network, zero-knowledge proof, NFC, communication, encryption, GUID.

Вступ

Провідні світові експерти з кібербезпеки визнають, що захист даних стає все більш критичним завданням у сучасному цифровому світі. Пірингові мережі, де учасники обмінюються даними без централізованого сервера, стають все більш популярними, але й роблять питання конфіденційності та безпеки ще більш гострими. При цьому пірингові мережі, дедалі більше стають мішенню для кіберзлочинців [1]. У таких умовах необхідно знайти надійні та ефективні методи захисту даних.

На сьогоднішній день дуже важливо приділити увагу захищеному обміну корпоративними даними, адже використання сторонніх ресурсів для комунікації може призвести до втрати або компрометації конфіденційних даних. Для цього використовуються пірингові мережі, що спрямовані на забезпечення цілісності, доступності та конфіденційності даних. Проте першочерговим постає питання захищеного обміну ідентифікаційними даними, оскільки це є першим кроком встановлення комунікації між двома вузлами у пірингові мережі [2]. Використання сторонніх ресурсів або центрального сервера є вразливістю, яка може спричинити небажані наслідки для корпоративних даних. Саме тому актуальним є питання захисту ідентифікаційних даних при їх передачі.

Результати дослідження

Обмін ідентифікаційними даними між вузлами є важливою передумовою для їхньої подальшої взаємодії. Іншими словами, поки обидва вузли в мережі не обміняються інформацією про свої адреси в мережі, ідентифікатори та ключі шифрування, не можна очікувати взаємного обміну комунікаційними даними.

Для забезпечення максимальної надійності та простоти використання при обміні даними, було обрано технологію NFC (Near Field Communication). NFC – це бездротова технологія ближнього зв’язку, яка працює на частоті 13,56 МГц та має малий радіус дії (до 4 см). Вона використовує стандарт радіоінтерфейсу ISO/IEC 18000-3 і забезпечує швидкість передачі даних від 106 до 848 кбіт/с [3]. Перевагами NFC є:

1. Висока надійність. NFC використовує шифрування та інші методи захисту даних, що робить його дуже безпечним способом обміну інформацією.

2. Простота використання. NFC не потребує спеціальних знань чи навичок для використання.
3. Швидкість. NFC дає змогу швидко обмінюватися даними.
4. Малий радіус дії. NFC робить перехоплення даних практично неможливим.

Для встановлення зв’язку між двома вузлами, вони повинні обмінятись такими даними, як ідентифікатор, ключі шифрування та адреса у мережі .Але для унеможливлення фальсифікації цих даних необхідно провести верифікацію за допомогою методу доказу нульового знання (ДНЗ) [4]. Це метод для доведення однією стороною іншій, що твердження (зазвичай математичне) є істинним, але без розкриття будь-якої іншої інформації, окрім достовірності твердження. Таким чином, виконуються наступні кроки:

1. Вузол, що ініціює встановлення з’єднання (далі Ініціатор) використовує NFC для надсилання службових даних про бажання встановлення з’єднання.
2. Вузол, з яким встановлюється з’єднання (далі Приймач) надсилає у відповідь підтвердження готовності. Якщо приймач не надсилає підтвердження готовності у чітко визначеному форматі та протягом часу $t = 5$ секунд, процес встановлення з'єднання припиняється. Це робиться для захисту від зловмисників, які можуть не знати про необхідність надсилання відповіді або намагатися імітувати приймача.
3. Ініціатор ділиться своїм публічним ключем з приймачем [5]. Якщо ініціатор не надсилає ключ, процес зупиняється, адже він може бути зловмисником. Ініціатор очікує час $t = 5$ секунд на отримання публічного ключа приймача. Публічні ключі обох учасників використовуються для шифрування даних під час з'єднання.
4. Приймач відповідає, надсилаючи свій публічний ключ. Якщо ключ не надходить протягом часу $t = 5$ секунд, процес зупиняється, адже приймач може бути зловмисником.
5. Далі починається процес верифікації методом ДНЗ:
    a. Ініціатор створює унікальний ідентифікатор GUID, який потім шифрується за допомогою публічного ключа приймача. Зашифрований ідентифікатор надсилається приймачу. GUID (Globally Unique Identifier) – це унікальний 128-бітовий код, який використовується для ідентифікації об'єктів або елементів у комп'ютерних системах. Він розроблений таким чином, щоб бути практично неповторним, що означає, що ймовірність появи двох однакових GUID є надзвичайно низькою [6].
    b. Приймач використовує свій приватний ключ для розшифрування повідомлення, а потім надсилає розшифроване повідомлення ініціатору.
    c. Ініціатор порівнює отриманий від приймача рядок з раніше згенерованим ідентифікатором. Якщо рядки не збігаються, процес припиняється, адже приймач може бути зловмисником, який не знає алгоритму верифікації.
    d. Після успішної верифікації приймача ініціатор надсилає йому повідомлення про підтвердження. Наступним кроком стає верифікація ініціатора.
    e. Приймач також створює унікальний ідентифікатор GUID, який шифрується за допомогою публічного ключа ініціатора. Приймач надсилає ці дані ініціатору.
    f. Ініціатор використовує свій приватний ключ для розшифрування повідомлення, а потім надсилає розшифроване повідомлення приймачу.
    g. Приймач порівнює отриманий рядок з раніше згенерованим ідентифікатором. Якщо рядки не збігаються, процес припиняється, адже ініціатор може бути зловмисником, який сфальсифікував результат.
6. Після завершення взаємної верифікації за допомогою методу доказу нульового знання, ініціатор надсилає приймачу свої ідентифікаційні дані.
7. Після отримання ідентифікаційних даних ініціатора, приймач ділиться власними, і обидві сторони стають безпосередніми учасниками пірингової мережі, вільно здійснюючи комунікацію.

На рисунку 1 наведено діаграму послідовностей, що описує розроблений метод.

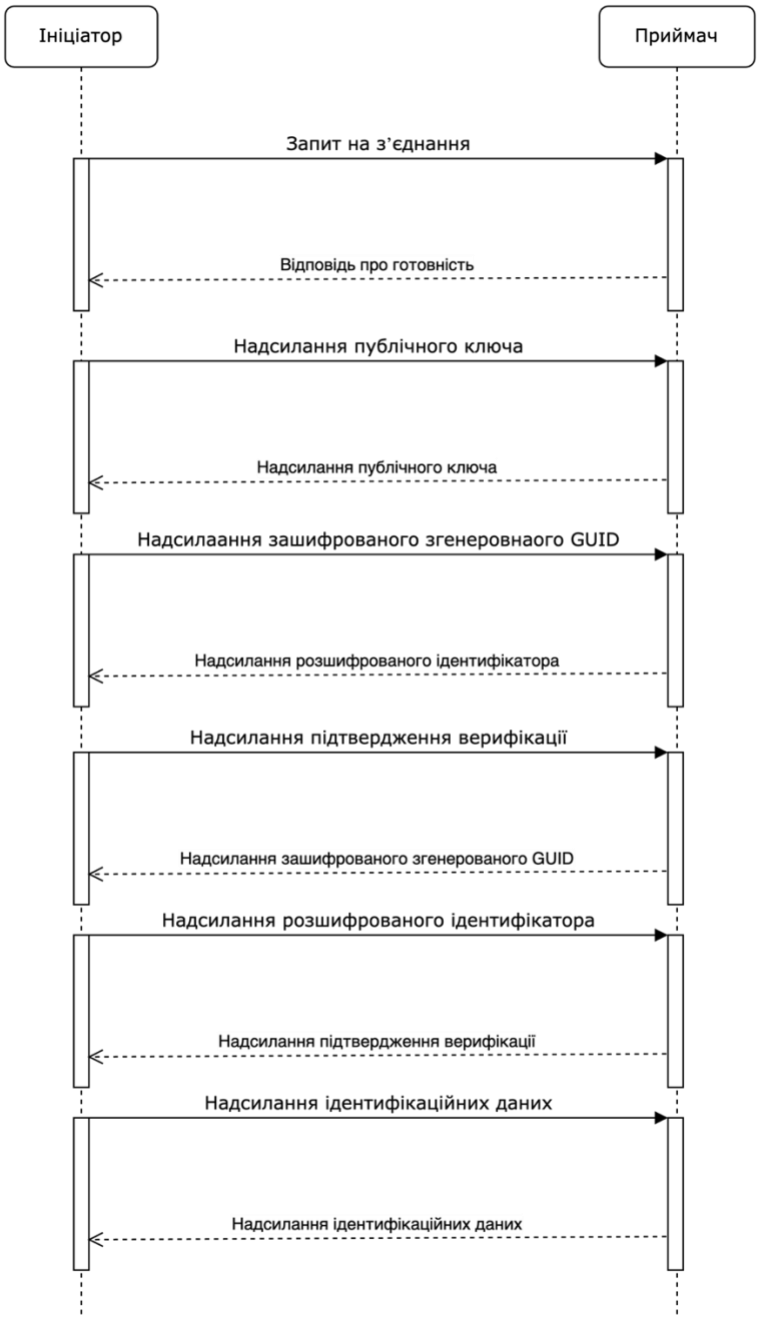

Рис. 1. Діаграма послідовностей обміну ідентифікаційними даними

Розроблений метод забезпечує:

1. Захист даних під час передачі. NFC використовує бездротовий зв'язок на короткій відстані (в межах кількох сантиметрів). Це дозволяє запобігти атакам, що базуються на віддаленому перехопленні даних.
2. Конфіденційність. Завдяки короткій дистанції передачі даних, ускладнюється їх перехоплення.
3. Аутентифікація. Використання доказу нульового знання через NFC може служити засобом підтвердження ідентичності користувачів, не викриваючи конкретну інформацію про їхні секрети. Це сприяє ефективній захисту вхідних точок до системи від несанкціонованого доступу.
4. Відмовостійкість. Якщо користувач володіє секретом, він може підтвердити свою ідентичність за допомогою доказу нульового знання через NFC. Це ускладнює можливість спростування факту володіння секретом після надання відповіді. Крім того, сама технологія NFC забезпечує достатньо високий рівень стійкості до відмов.

5. Захист від атак з перехопленням трафіку. Застосування технології NFC може захистити від атак типу "Людина посередині", оскільки передача даних відбувається на дуже короткій відстані, що робить перехоплення трафіку важким завданням, особливо без посередників.

6. Надійність верифікації. Оскільки для верифікації використовується GUID як дані, що передаються, то імовірність того, що ініціатор чи приймач зможуть випадково вибрати або вгадати таке саме значення, майже нульова. Забезпечується це тим, що загальна кількість унікальних GUID 2^128=3,4028*10^38.

Висновки

Запропоновано метод безпечного обміну ідентифікаційними даними між двома вузлами, який поєднує NFC для передачі даних та поетапну верифікацію за допомогою методу доказу нульового знання. Цей метод гарантує безпечний та ефективний обмін ідентифікаційними даними в піринговых мережах. Обмеженням запропонованого методу є те, що обмін даними можливий лише за допомогою пристроїв, що підтримують технологію NFC, а також те, що двом вузлам необхідна безпосередня фізична близькість (відстань між пристроями повинна бути не більша 4 см). Проте даний метод орієнтований на захищеність встановлення корпоративної комунікації, де працівники можуть використати свої пристрої для обміну через NFC.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A Survey of P2P Network Security. arXiv.org. URL: https://doi.org/10.48550/arXiv.1504.01358 (дата звернення: 15.03.2024).

2. Ryan Randy Suryono, Betty Purwandari, Indra Budi. Peer to Peer (P2P) Lending Problems and Potential Solutions: A Systematic Literature Review. The Fifth Information Systems International Conference, Surabaya, Indonesia, 23-24 July 2019. DOI:10.1016/j.procs.2019.11.116

3. Jain, Garima. NFC: Advantages, limits and future scope / International Journal on Cybernetics & Informatics. 2021. Vol. 4 P. 12.

4. P.Lalitha Surya Kumari, C.H.Sarada devi, S. Thivaharan, K. Srinivas, Avula Damodaram. A resilient group session key authentication methodology for secured peer to peer networks using zero knowledge protocol / Optik. 2023. Vol. 273. P.30 URL: https://www.sciencedirect.com/science/article/abs/pii/S0030402622016035

5. Exploring E2EE: Real-world Examples of End-to-End Encryption. Kiteworks | Your Private Content Network. URL: https://www.kiteworks.com/secure-file-sharing/real-world-examples-of-end-to-end-encryption (дата звернення: 15.03.2024).

6. Властивість «Глобальний унікальний ідентифікатор» (GUID) - Підтримка від Microsoft. Microsoft Support. URL: https://support.microsoft.com/uk-ua/topic/властивість-глобальний-унікальний-ідентифікатор-guid-a4caad5d-7a8a-43e5-89f4-d2afad92bab8 (дата звернення: 15.03.2024).

Кренцін Михайло Дмитрович — аспірант кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: mishatron98@gmail.com

Куперштейн Леонід Михайлович — канд. техн. наук, доцент кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: kupershtein.lm@gmail.com

Krentsin Mykhailo D. — postgraduate student of the Department of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: mishatron98@gmail.com

Kupershtein Leonid M. — Ph.D. technical of Sciences, Associate Professor of the Department of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: kupershtein.lm@gmail.com