КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.7988
УДК 004.056

Кренцін Михайло Дмитрович
аспірант кафедри захисту інформації
Вінницький національний технічний університет, Вінниця, Україна
ORCID ID: 0000-0002-1792-9401
mishatron98@gmail.com

Куперштейн Леонід Михайлович
к.т.н., доцент кафедри захисту інформації
Вінницький національний технічний університет, Вінниця, Україна
ORCID ID: 0000-0001-6737-7134
kupershtein.lm@gmail.com

МЕТОД ОБМІНУ ІДЕНТИФІКАЦІЙНИМИ ДАНИМИ МІЖ ВУЗЛАМИ ПІРИНГОВОЇ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ NFC

Анотація. Останнє десятиліття змінило тренди використання пірингових мереж. Однією із сфер використання P2P мереж є комунікація між людьми. На сьогоднішній день дуже важливим є те, щоб комунікація була максимально захищена, особливо якщо вона здійснюється між працівниками підприємства, адже кількість кіберзагроз постійно зростає. Сучасні підходи до захищеності пірингових мереж полягають у шифруванні даних, автентифікації вузлів, виявлення та запобігання шкідливих вузлів, обмеження доступу, моніторингу трафіку тощо. Проте одним із найперших кроків є саме обмін ідентифікаційними даними, і цей процес повинен бути максимально надійним та захищеним. У статті запропоновано метод захищеного обміну ідентифікаційними даними між вузлами пірингової мережі, що базується на використанні технології NFC у поєднанні з доказом нульового знання. NFC використовується для безпосереднього обміну даними по радіоінтерфейсу, що завдяки малому радіусу дії знижує ризик перехоплення даних. Для встановлення з'єднання вузли повинні обмінятись ідентифікаторами, публічними ключами шифрування та адресами у мережі. Для того, щоб виявити чи вузол не є зловмисним, передбачається взаємна верифікація вузлів за допомогою доказу нульового знання. У якості секрету, що не розголошується виступає згенерований кожним з вузлів унікальний ідентифікатор типу GUID. Вузли спочатку обмінюються публічними ключами, якими шифрують ідентифікатори і обмінюються ними. Після розшифрування своїми приватними ключами вузли перевіряють чи отримане значення дорівнює початковому. У випадку рівності значень вузли є взаємно верифікованими і обмінюються ідентифікаційними даними. Запропонований у статті метод спрямований на забезпечення відмовостійкості та конфіденційності. Також передбачається захист від атак з перехопленням трафіку та надійність процесу верифікації.

Ключові слова: пірингова мережа; NFC; шифрування; верифікація; доказ нульового знання; ідентифікатор; GUID; RSA.

ВСТУП

Останнє десятиліття змінило тренди використання пірингових мереж. Однією із сфер використання P2P мереж є комунікація між людьми. В умовах зростаючої кількості кіберзагроз комунікація повинна бути максимально надійна та захищена, особливо у випадках, коли йдеться про обмін даними між працівниками підприємства, адже витік конфіденційної інформації може спричинити небажані для підприємства наслідки.

Для забезпечення конфіденційності корпоративних даних використовуються пірингові мережі (P2P), що спрямовані на забезпечення цілісності, доступності та конфіденційності обмінюваних даних.

Пірингова мережа (Peer-to-peer, P2P) — це мережа рівноправних вузлів, де відсутній центральний сервер [1]. Це означає, що кожен вузол у мережі має рівний статус і може одночасно виконувати роль клієнта та сервера, обмінюючись даними без посередництва центрального вузла.

У контексті корпоративної комунікації, пірингові мережі використовуються для різних цілей, включаючи обмін файлами (особливо великими), відеоконференції, спільну роботу над документами, ефективне використання ресурсів тощо [2]. Отже, впровадження пірингових мереж у корпоративну комунікацію є важливим кроком для забезпечення надійного, безпечного та ефективного обміну даними між працівниками підприємства, оскільки працівники обмінюються різноманітною конфіденційною інформацією.

Постановка проблеми. Основною проблемою P2P-мереж є те, що через їхню децентралізовану структуру безпека не може бути забезпечена таким чином, що й при клієнт-серверній архітектурі. Захищеність пірингових мереж досягається за рахунок шифрування даних, автентифікації вузлів, виявлення та запобігання шкідливої активності вузлів, обмеження доступу, моніторингу трафіку тощо [3].

Одним із важливих аспектів забезпечення безпечної комунікації вузлів пірингової мережі є захищений обмін ідентифікаційними даними, оскільки це є наступним кроком після автентифікації (рис. 1) [4]. Для того, щоб два вузли могли здійснювати комунікацію, спочатку кожен з них повинен пройти автентифікацію. Після чого вони повинні обмінятись ідентифікаційними даними. Далі вузли можуть встановити з’єднання та розпочати обмін даними.

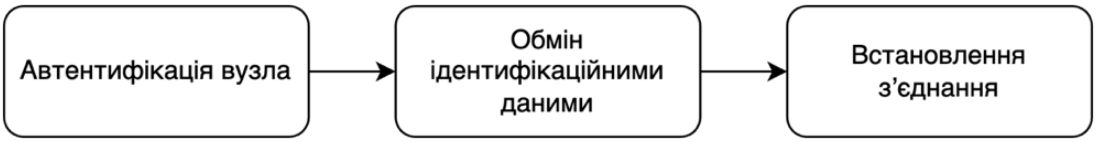

Рис. 1. Необхідні кроки перед початком комунікації

У пірингових мережах існує кілька підходів до обміну ідентифікаційними даними між вузлами, аби вони могли далі здійснювати комунікацію. Кожен з них має свою специфіку, переваги та недоліки.

1. Мережа довіри. Основна ідея полягає в тому, щоб вузли могли перевіряти та підтверджувати ідентичність один одного на основі певних параметрів або спостережень [5]. Підхід є ефективним, проте потребує певну систему репутації (рейтингу), на основі якої можна визначити чи два вузли мережі можуть здійснити подальшу комунікацію. Певний рівень рейтингу вузол може мати після певного часу користування мережею, а тому даний метод обмежений на початку входження нового вузла у мережу. Також підхід не гарантує, що довірений вузол не є зловмисним.

2. Децентралізована автентифікація. Вузли можуть використовувати криптографічні методи для здійснення автентифікації і подальшого обміну ідентифікаційними даними. Перевагою є конфіденційність, що забезпечується відсутністю посередників. Проте даний підхід не передбачує перевірку автентичності

вузла, тобто те чи є вузол тим, за кого себе видає. Це пов'язано з тим, що у пірингових мережах немає єдиного джерела правди.

3. Використання стороннього програмного забезпечення. Передбачає використання сторонніх програм та каналів зв'язку для надсилання ідентифікаційних даних між двома користувачами. Перевагою є простота використання. Проте такий підхід не є конфіденційним, оскільки присутня третя сторона, яка може отримати ці дані.

4. Використання центрального серверу. Передбачає створення гібридної пірингової мережі, де центральний сервер може виконувати певні задачі, як от, наприклад, збереження на надання вузлам ідентифікаційних даних інших вузлів. Перевагою є простота реалізації, проте підхід не забезпечує відмовостійкість та конфіденційність даних.

5. Ручний обмін. Передбачає ручне внесення усіх необхідних даних у програмне забезпечення мережі з метою подальшої комунікації з певним вузлом. Забезпечує високий рівень конфіденційності, проте є незручним у використанні та існує вірогідність людської помилки при введенні даних.

Кожен з цих підходів має свої переваги та недоліки і може бути використаний залежно від потреб і вимог конкретної пірингової мережі. Проте, враховуючи переваги та недоліки вищеописаних підходів та необхідність забезпечити максимальну надійність при обміні, конфіденційність та простоту у використанні, було прийнято рішення взяти за основу технологію NFC (Near Field Communication) [6].

NFC — це технологія бездротового зв'язку малого радіусу дії (до 4 сантиметрів). NFC використовує частоту 13,56 МГц та базується на індуктивному зв'язку між двома електромагнітними котушками. Стандарти NFC охоплюють протоколи зв'язку та формати обміну даними та базуються на існуючих стандартах радіочастотної ідентифікації (RFID), включаючи ISO/IEC 14443 і FeliCa. Стандарти включають ISO/IEC 18092 і стандарти, визначені «Форумом NFC» [7]. Обмін даними відбувається зі швидкістю передачі від 106 до 424 кбіт/с. Основне призначення NFC — швидкий обмін невеликими фрагментами інформації, такими як контактна інформація або ключі шифрування.

На сьогоднішній день більше половини усієї комунікації відбувається за допомогою мобільних пристроїв [8]. На 2023 рік кількість користувачів смартфонів перевищила 6 мільярдів. Це означає, що понад 75% населення Землі користується смартфонами. Також переважна більшість мобільних телефонів оснащена технологією NFC, що дозволяє більшості користувачі здійснювати обмін ідентифікаційними даними. Проте актуальним є розробка методу здійснення обміну ідентифікаційними даними, що буде забезпечувати відмовостійкість, конфіденційність та простоту у використанні. Необхідно також врахувати загрози, як наприклад перехоплення сигналу (хоча NFC працює на короткій відстані, зловмисник може використовувати спеціальне обладнання для перехоплення сигналу) чи атаки відтворення (зловмисник може записати транзакцію і спробувати повторити її пізніше, якщо не використовується належний механізм захисту) [9]. Тому необхідно передбачити шифрування даних при обміні ідентифікаційними даними. Єдиним обмеженням методу є необхідність безпосередньої фізичної близькості вузлів (мобільних пристроїв) та підтримка NFC самими пристроєм, проте це не є завадою в контексті корпоративної комунікації, оскільки даними вузли повинні обмінятись лише один раз і ця фізична близькість є можливою на підприємстві.

Аналіз останніх досліджень і публікацій. На сьогоднішній день підвищення захищеності пірингових мереж залишається актуальною темою досліджень. Останні дослідження та публікації, присвячені підвищенню захищеності пірингових мереж,

відображають загальний інтерес у забезпеченні безпеки та приватності користувачів у цих мережах. Деякі ключові напрями цих досліджень включають такі аспекти:

1. Криптографічні методи. В сучасних дослідженнях активно досліджується використання сучасних криптографічних методів для захисту комунікацій у пірингових мережах [10], [11]. Це включає розробку нових протоколів шифрування та автентифікації, таких як методи застосування доказу нульового знання та криптографічні алгоритми з підтримкою квантових технологій.

2. Автентифікація. Деякі дослідження фокусуються на розробці методів автентифікації вузлів у пірингових мережах, оскільки методи, що використовуються у клієнт-серверній взаємодії не підходять для P2P [12], [13].

3. Захист від атак та вразливостей. Інші дослідження спрямовані на виявлення та запобігання атакам у пірингових мережах, таким як атаки перехоплення даних, атаки з підробки даних та атаки на протоколи обміну інформацією [14], [15]. Це включає розробку ефективних механізмів виявлення та відновлення після атак.

4. Інтеграція з новими технологіями. Деякі дослідження досліджують можливості інтеграції пірингових мереж з новими технологіями, такими як розподілені обчислення. Це може забезпечити додаткові шари безпеки та прозорості для пірингових мереж [16], [17].

Існують також дослідження, пов’язані із використанням NFC:

1. P2P платежі — здійснення прямих фінансових транзакцій між користувачами без необхідності проходження через централізовану фінансову установу [18], [19].
2. Обмін даними за допомогою NFC (наприклад обмін зображеннями) [20].
3. Взаємодія мобільного телефону із медичними сенсорами [21].

В цілому, останні дослідження та публікації підтверджують постійний інтерес до підвищення захищеності пірингових мереж і вказують на широкий спектр стратегій та методів, які використовуються для цієї мети. Також практичний інтерес до технології NFC свідчить про потенційні перспективи її застосування у організації роботи корпоративних пірингових мереж.

Метою дослідження є підвищення захищеності пірингових мереж за рахунок захищеного обміну ідентифікаційними даними з використанням технології NFC.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для того, щоб встановити зв’язок вузли повинні обмінятись ідентифікаційними даними $DATA = \{id, k^{pub}, addr\}$, що включають в себе ідентифікатор вузла id, публічний ключ (яким будуть шифруватись в подальшому обмінювані дані) k^{pub} та IP-адресу $addr$. Але для унеможливлення фальсифікації цих даних пропонується провести верифікацію за допомогою доказу нульового знання (ДНЗ) [22]. ДНЗ є методом, який дозволяє одній стороні підтвердити іншій, що вона володіє певними даними, не розкриваючи самі ці дані.

Нехай є ініціатор I — вузол, що ініціює з’єднання для обміну; та приймач R — вузол, з яким встановлюється з’єднання. Ініціатор I має публічний ключ k_I^{pub} та приватний ключ k_I^{pr}, що генеруються під час першої автентифікації вузла (тобто тоді, коли вузол перший раз приєднується до пірингової мережі). Для генерації ключів та шифрування використовується алгоритм RSA [23] із генерацією простого числа довжиною 2048 біт, що зумовлено сучасними вимогами до безпеки [24]. Це пов’язано із тим, що RSA забезпечує високий рівень безпеки, є частиною багатьох криптографічних

стандартів, забезпечує високий рівень ефективності, а також його безпека була підтверджена численними тестами та аудитами. Приймач має публічний ключ k_R^{pub} та приватний ключ k_R^{pr}. Максимальний час очікування відповіді вузлом на кожному кроці становить tw після чого процес припиняється, оскільки приймач чи ініціатор може бути зловмисником. Також процес припиняється у випадку, якщо надіслані дані є хибними (невірний формат, невірна відповідь, надлишкові дані).

Метод обміну ідентифікаційними даними передбачає виконання наступних кроків

1. Ініціатор I за допомогою NFC надсилає приймачу запит на встановлення з'єднання SD.

2. Приймач R надсилає у відповідь підтвердження готовності SR.

3. Ініціатор I генерує тимчасову пару ключів (публічний та приватний) kt_I^{pub}, kt_I^{pr} та надсилає приймачу R свій публічний ключ kt_I^{pub}.

4. Приймач R генерує тимчасову пару ключів (публічний та приватний) kt_R^{pub}, kt_R^{pr} та надсилає ініціатору I свій публічний ключ kt_R^{pub}. Після цього починається процес верифікації.

5. За допомогою ДНЗ розпочинається взаємна верифікація вузлів, що представлена наступною формулою:

$$VR = V(I, R), \tag{1}$$

де V — функція верифікації, $VR = 1$ — успішний та $VR = 0$ неуспішний результат верифікації.

5.1. Спочатку ініціатор I генерує унікальний ідентифікатор ID_I типу GUID [25]. Далі цей ідентифікатор зашифровується за допомогою публічного ключа приймача kt_R^{pub} і результат RE_I надсилається приймачу R. Функцію шифрування можна подати наступним чином:

$$RE_I = E(ID_I, kt_R^{pub}), \tag{2}$$

де RE_I — результат функції шифрування, а E — сама функція шифрування.

5.2. Приймач R розшифровує повідомлення RE_I за допомогою свого приватного ключа kt_R^{pr}. В результаті отримуємо функцію розшифрування, що представлена формулою

$$RD_R = D(RE_I, kt_R^{pr}), \tag{3}$$

де D — функція розшифрування, а RD_R — результат розшифрування, що й надсилається у відповідь ініціатору I.

5.3. Ініціатор I порівнює отримане від приймача R значення з згенерованим у кроці 5.1. Таким чином, якщо $RD_R = ID_R$, то ініціатор I надсилає приймачу відповідь про його успішну верифікацію VS_R і процес продовжується далі.

5.4. Приймач R генерує унікальний ідентифікатор ID_R типу GUID. Далі цей ідентифікатор зашифровується за допомогою публічного ключа ініціатора kt_I^{pub} і результат надсилається ініціатору I. Таким чином, маємо функцію шифрування:

$$RE_R = E(ID_R, kt_I^{pub}), \tag{4}$$

де RE_R — результат функції шифрування, а E — сама функція шифрування.

5.5. Ініціатор I розшифровує повідомлення RE_I за допомогою свого приватного ключа kt_I^{pr}. В результаті отримуємо функцію розшифрування

$$RD_I = D(RE_R, kt_I^{pr}), \tag{5}$$

де D — функція розшифрування, а RD_I — результат розшифрування, що й надсилається у відповідь приймачу.

ISSN 2663 - 4023

5.6. Приймач R порівнює отримане від ініціатора I значення з згенерованим у кроці 5.4. Таким чином, якщо $RD_I = ID_R$, то приймач R надсилає ініціатору I відповідь про його успішну верифікацію VS_I і процес продовжується далі.

6. Ініціатор I надсилає приймачу R свої ідентифікаційні дані $DATA_I$ і очікує такі ж від приймача R:

$$DATA_I = \{id_I, k_I^{pub}, addr_I\}, \quad (6)$$

7. Приймач R надсилає ініціатору I свої ідентифікаційні дані $DATA_R$, після чого процес зупиняється після успішного виконання:

$$DATA_R = \{id_R, k_R^{pub}, addr_R\}, \quad (7)$$

Отже, після усіх семи кроків вузли є безпосередніми учасниками піринговоі мережі та можуть здійснювати подальшу комунікацію. На рис. 2 представлена діаграма послідовностей, що описує весь процес обміну.

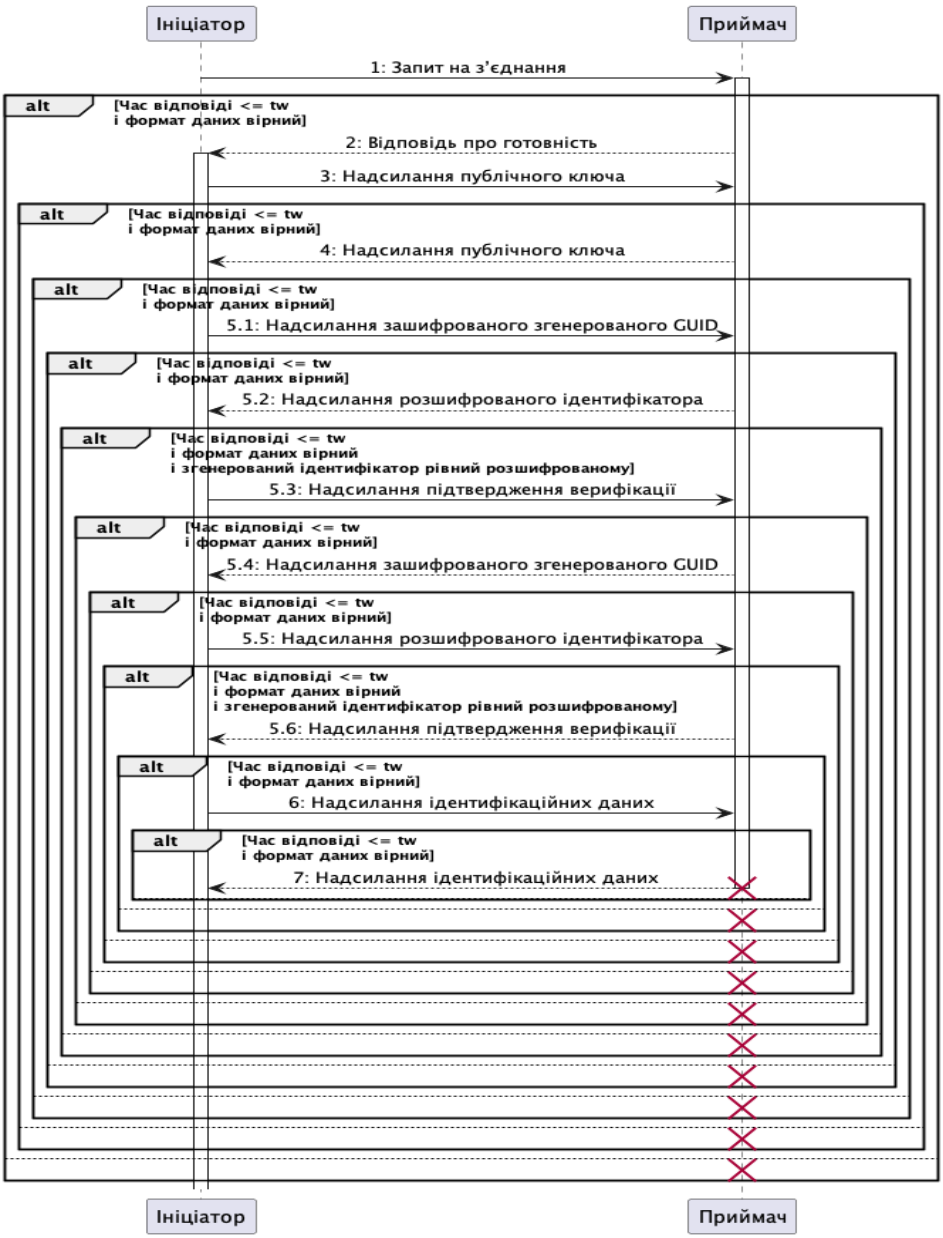

Рис. 2. UML-діаграма процесу обміну ідентифікаційними даними

Розроблений метод забезпечує наступні показники захищеності:

1. Конфіденційність. Завдяки короткій дистанції передачі даних, їх важко підслухати. Це дозволяє захистити конфіденційні дані, якими обмінюються сторони.

2. Відмовостійкість. Сама технологія NFC забезпечує досить високий рівень відмовостійкості.

3. Надійність верифікації. Оскільки даними, що верифікуються є ідентифікатори GUID, то імовірність того, що зловмисний вузол зможе підібрати ці значення близька до нуля завдяки тому, що загальна кількість унікальний GUID дорівнює 2^{128}.

4. Захист від атак з перехопленням трафіку. Це досягається за рахунок того, що при обміні даними не використовується сама мережа чи Інтернет загалом, а також завдяки малому радіусу дії технології NFC, що передбачає безпосередню фізичну близькість вузлів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Розглянуто поняття пірингових мереж, їх використання, а також необхідність ефективних механізмів їх захисту.

Розглянуто технологію NFC як швидкий та безпечний спосіб обміну даними. Досягається це за рахунок використання індуктивного зв'язку малого радіусу дії та радіочастотної ідентифікації.

Запропоновано метод застосування технології NFC для захищеного обміну ідентифікаційними даними між вузлами пірингової мережі. Обмеженням даного методу є те, що вузлам необхідна безпосередня фізична близькість на момент самого обміну. Проте у випадку використання методу для працівників підприємства це не є завадою.

У подальших досліджень передбачається аналіз та розробка інших методів підвищення захищеності пірингових мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Куперштейн, Л. М., Кренцін, М. Д., Дудатьєв, А. В., & Каплун, В. А. (2022). Аналіз проблем безпеки пірингових мереж. *Інформаційні технології та комп'ютерна інженерія*, *54(2),* 5–14. https://doi.org/10.31649/1999-9941-2022-54-2-5-14
2. Ismail, A., & Kastner, W. (2016). Co-operative peer-to-peer systems for industrial middleware. *2016 IEEE World Conference on Factory Communication Systems (WFCS).* https://doi.org/10.1109/wfcs.2016.7496497
3. Qureshi, H. (2019). *P2P Networking*. NAKAMOTO. https://nakamoto.com/p2p-networking
4. Suryono, R. R., Purwandari, B., & Budi, I. (2019). Peer to Peer (P2P) Lending Problems and Potential Solutions: A Systematic Literature Review. *Procedia Computer Science*, *161,* 204–214. https://doi.org/10.1016/j.procs.2019.11.116
5. Tennakoon, P., Karunathilaka, S., Lavakumar, R., Alawatugoda, J., & Alawatugoda, J. (2023). Anonymous and Distributed Authentication for Peer-to-Peer Networks. *Journal of Computer Science, 19(1),* 1–10. https://doi.org/10.3844/jcssp.2023.1.10
6. Jain, G., & Dahiya, S. (2015). NFC: Advantages, Limits and Future Scope. *International Journal on Cybernetics & Informatics, 4(4),* 1–12. https://doi.org/10.5121/ijci.2015.4401
7. *ISO/IEC 18092:2023*. ISO. https://www.iso.org/standard/82095.html
8. *64% українців замінюють живе спілкування на віртуальне @ Закарпаття онлайн.* Новини Закарпаття онлайн, новини Ужгорода, новости Закарпатья онлайн. https://zakarpattya.net.ua/News/111470-64-ukraintsiv-zaminiuiut-zhyve-spilkuvannia-na-virtualne

9. Chen, C. H., Lin, I. C., & Yang, C. C. (2014). NFC Attacks Analysis and Survey. *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*. https://doi.org/10.1109/imis.2014.66
10. Jawad, M., Serrano-Alvarado, P., & Valduriez, P. (2009). Protecting Data Privacy in Structured P2P Networks. *Lecture Notes in Computer Science*, 85–98. https://doi.org/10.1007/978-3-642-03715-3_8
11. Wang, E. K., Ye, Y., Yiu, S. M., & Hui, L. C. K. (2013). Privacy-Preserving P2P Information Sharing Protocol for Mobile Social Networks. *International Journal of Computer and Communication Engineering*, 338–342. https://doi.org/10.7763/ijcce.2013.v2.200
12. Wang, X., Yang, L., Sun, X., Han, J., Liang, W., & Huang, L. (2010). Survey of Anonymity and Authentication in P2P Networks. *Information Technology Journal*, *9(6)*, 1165–1171. https://doi.org/10.3923/itj.2010.1165.1171
13. Jagdale, B. N., & Bakal, J. W. (2020). A novel authentication and authorization scheme in P2P networking using location-based privacy. *Evolutionary Intelligence*. https://doi.org/10.1007/s12065-020-00375-y
14. Xu, X., Lu, H., & Chen, L. (2014). Defending Against sybil-attacks in Peer-to-Peer Networks. *International Journal of Security and Its Applications*, *8(4)*, 329–340. https://doi.org/10.14257/ijsia.2014.8.4.30
15. Folino, F., Folino, G., Pontieri, L., & Sabatino, P. (2017). A Peer-to-Peer Architecture for Detecting Attacks from Network Traffic and Log Data. *2017 International Conference on High Performance Computing & Simulation (HPCS)*. https://doi.org/10.1109/hpcs.2017.116
16. Куперштейн, Л. М., & Кренцін, М. Д. (2021). Аналіз тенденцій розвитку пірингових мереж. *Вісник Хмельницького національного університету*, *299(4)*, 26–29. https://doi.org/10.31891/2307-5732-2021-299-4-26-29
17. Yin, K., Huang, H., Cohen-Or, D., & Zhang, H. (2018). P2P-NET. *ACM Transactions on Graphics*, *37(4)*, 1–13. https://doi.org/10.1145/3197517.3201288
18. Monteiro, D. M., Rodrigues, J. J. P. C., Lloret, J., & Sendra, S. (2013). A hybrid NFC-Bluetooth secure protocol for Credit Transfer among mobile phones. *Security and Communication Networks*, *7(2)*, 325–337. https://doi.org/10.1002/sec.732
19. Abouhogail, R. A. (2022). A New Secure Lightweight Authentication Protocol for NFC mobile Payment. *International Journal of Communication Networks and Information Security (IJCNIS)*, *11(2)*. https://doi.org/10.17762/ijcnis.v11i2.4142
20. Seewoonauth, K., Rukzio, E., Hardy, R., & Holleis, P. (2009). Two NFC interaction techniques for quickly exchanging pictures between a mobile phone and a computer. *11th International Conference*. ACM Press. https://doi.org/10.1145/1613858.1613909
21. Zhang, H., & Li, J. (2011). NFC in medical applications with wireless sensors. У 2011 *International Conference on Electrical and Control Engineering (ICECE)*. https://doi.org/10.1109/iceceng.2011.6057534
22. Kumari, P. L. S., devi, C. H. S., Thivaharan, S., Srinivas, K., & Damodaram, A. (2022). A Resilient Group Session Key Authentication Methodology for Secured Peer to Peer Networks using Zero Knowledge Protocol. *Optik*, *170345*. https://doi.org/10.1016/j.ijleo.2022.170345
23. Nemec, M., Sys, M., Svenda, P., Klinec, D., & Matyas, V. (2017). The Return of Coppersmith's Attack. *CCS '17: 2017 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/3133956.3133969
24. Barker, E. B., & Dang, Q. H. (2015). *Recommendation for Key Management Part 3: Application-Specific Key Management Guidance*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-57pt3r1
25. *RFC 4122: A Universally Unique IDentifier (UUID) URN Namespace.* IETF Datatracker. https://datatracker.ietf.org/doc/html/rfc4122

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Mykhailo Krentsin
PhD student of Information Protection Department
Vinnytsia national technical University, Vinnytsia, Ukraine
ORCID ID: 0000-0002-1792-9401
mishatron98@gmail.com

Leonid Kupershtein
PhD, Associate Professor of Information Protection Department
Vinnytsia national technical University, Vinnytsia, Ukraine
ORCID ID: 0000-0001-6737-7134
kupershtein.lm@gmail.com

NFC TECHNOLOGY AS A MEANS OF PROTECTED EXCHANGE OF IDENTIFICATION DATA BETWEEN PEER-TO-PEER NETWORK NODES

Abstract. The last decade has changed the trends of using peering networks. One of the areas of use of P2P networks is communication between people. Today, it is very important that communication is as protected as possible, especially if it is carried out between employees of the enterprise, because the number of cyber threats is constantly increasing. Modern approaches to the security of peering networks consist of data encryption, node authentication, detection and prevention of malicious nodes, access restriction, traffic monitoring, etc. However, one of the very first steps is the exchange of identification data itself, and this process must be as secure and secure as possible. The article proposes a method of secure exchange of identification data between peering network nodes, based on the use of NFC technology in combination with proof of zero knowledge. NFC is used for direct data exchange over the radio interface, which, thanks to its short range, makes it impossible to intercept data. To establish a connection, nodes must exchange identifiers, public encryption keys, and network addresses. In order to find out whether a node is not malicious, mutual verification of nodes using zero-knowledge proof is assumed. A unique identifier of the GUID type generated by each of the nodes acts as a secret that is not disclosed. Nodes first exchange public keys that encrypt and exchange identifiers. After decryption with their private keys, the nodes check whether the received value is equal to the initial one. In case of equality of values, the nodes are mutually verified and exchange identification data. The method proposed in the article is aimed at ensuring fault tolerance and confidentiality. It also provides protection against traffic interception attacks and the reliability of the verification process.

Keywords: peer-to-peer network; NFC; encryption; verification; zero knowledge proof; identifier; GUID; RSA.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kupershtein, L. M., Krentsin, M. D., Dudatyev, A. V., & Kaplun, V. A. (2022). Analysis of Security Problems of Peer-To-Peer Networks. *Information technology and computer engineering*, *54(2)*, 5–14. https://doi.org/10.31649/1999-9941-2022-54-2-5-14
2. Ismail, A., & Kastner, W. (2016). Co-operative peer-to-peer systems for industrial middleware. *2016 IEEE World Conference on Factory Communication Systems (WFCS)*. https://doi.org/10.1109/wfcs.2016.7496497
3. Qureshi, H. (2019). *P2P Networking*. NAKAMOTO. https://nakamoto.com/p2p-networking
4. Suryono, R. R., Purwandari, B., & Budi, I. (2019). Peer to Peer (P2P) Lending Problems and Potential Solutions: A Systematic Literature Review. *Procedia Computer Science*, *161*, 204–214. https://doi.org/10.1016/j.procs.2019.11.116
5. Tennakoon, P., Karunathilaka, S., Lavakumar, R., Alawatugoda, J., & Alawatugoda, J. (2023). Anonymous and Distributed Authentication for Peer-to-Peer Networks. *Journal of Computer Science*, *19(1)*, 1–10. https://doi.org/10.3844/jcssp.2023.1.10
6. Jain, G., & Dahiya, S. (2015). NFC: Advantages, Limits and Future Scope. *International Journal on Cybernetics & Informatics, 4(4),* 1–12. https://doi.org/10.5121/ijci.2015.4401

7. *ISO/IEC 18092:2023*. ISO. https://www.iso.org/standard/82095.html
8. *64% of Ukrainians replace live communication with virtual @ Transcarpathia online*. Zakarpattia news online, Uzhgorod news, Zakarpattia news online. https://zakarpattya.net.ua/News/111470-64-ukraintsiv-zaminiuiut-zhyve-spilkuvannia-na-virtualne
9. Chen, C. H., Lin, I. C., & Yang, C. C. (2014). NFC Attacks Analysis and Survey. *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*. https://doi.org/10.1109/imis.2014.66
10. Jawad, M., Serrano-Alvarado, P., & Valduriez, P. (2009). Protecting Data Privacy in Structured P2P Networks. *Lecture Notes in Computer Science*, 85–98. https://doi.org/10.1007/978-3-642-03715-3_8
11. Wang, E. K., Ye, Y., Yiu, S. M., & Hui, L. C. K. (2013). Privacy-Preserving P2P Information Sharing Protocol for Mobile Social Networks. *International Journal of Computer and Communication Engineering*, 338–342. https://doi.org/10.7763/ijcce.2013.v2.200
12. Wang, X., Yang, L., Sun, X., Han, J., Liang, W., & Huang, L. (2010). Survey of Anonymity and Authentication in P2P Networks. *Information Technology Journal*, *9(6)*, 1165–1171. https://doi.org/10.3923/itj.2010.1165.1171
13. Jagdale, B. N., & Bakal, J. W. (2020). A novel authentication and authorization scheme in P2P networking using location-based privacy. *Evolutionary Intelligence*. https://doi.org/10.1007/s12065-020-00375-y
14. Xu, X., Lu, H., & Chen, L. (2014). Defending Against sybil-attacks in Peer-to-Peer Networks. *International Journal of Security and Its Applications*, *8(4)*, 329–340. https://doi.org/10.14257/ijsia.2014.8.4.30
15. Folino, F., Folino, G., Pontieri, L., & Sabatino, P. (2017). A Peer-to-Peer Architecture for Detecting Attacks from Network Traffic and Log Data. *2017 International Conference on High Performance Computing & Simulation (HPCS)*. https://doi.org/10.1109/hpcs.2017.116
16. Kupershtein, L. M, Krentsin, M. D. (2021). Analysis of peer-to-peer networks trends. *Herald of Khmelnytskyi national university*, *299(4)*, 26–29. https://doi.org/10.31891/2307-5732-2021-299-4-26-29
17. Yin, K., Huang, H., Cohen-Or, D., & Zhang, H. (2018). P2P-NET. *ACM Transactions on Graphics*, *37(4)*, 1–13. https://doi.org/10.1145/3197517.3201288
18. Monteiro, D. M., Rodrigues, J. J. P. C., Lloret, J., & Sendra, S. (2013). A hybrid NFC-Bluetooth secure protocol for Credit Transfer among mobile phones. *Security and Communication Networks*, *7(2)*, 325–337. https://doi.org/10.1002/sec.732
19. Abouhogail, R. A. (2022). A New Secure Lightweight Authentication Protocol for NFC mobile Payment. *International Journal of Communication Networks and Information Security (IJCNIS)*, *11(2)*. https://doi.org/10.17762/ijcnis.v11i2.4142
20. Seewoonauth, K., Rukzio, E., Hardy, R., & Holleis, P. (2009). Two NFC interaction techniques for quickly exchanging pictures between a mobile phone and a computer. *11th International Conference*. ACM Press. https://doi.org/10.1145/1613858.1613909
21. Zhang, H., & Li, J. (2011). NFC in medical applications with wireless sensors. У 2011 *International Conference on Electrical and Control Engineering (ICECE)*. https://doi.org/10.1109/iceceng.2011.6057534
22. Kumari, P. L. S., devi, C. H. S., Thivaharan, S., Srinivas, K., & Damodaram, A. (2022). A Resilient Group Session Key Authentication Methodology for Secured Peer to Peer Networks using Zero Knowledge Protocol. *Optik*, *170345*. https://doi.org/10.1016/j.ijleo.2022.170345
23. Nemec, M., Sys, M., Svenda, P., Klinec, D., & Matyas, V. (2017). The Return of Coppersmith's Attack. *CCS '17: 2017 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/3133956.3133969
24. Barker, E. B., & Dang, Q. H. (2015). *Recommendation for Key Management Part 3: Application-Specific Key Management Guidance*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-57pt3r1
25. *RFC 4122: A Universally Unique IDentifier (UUID) URN Namespace.* IETF Datatracker. https://datatracker.ietf.org/doc/html/rfc4122