УДК 621.311.1.018.3

М. Д. Кренцін; Л. М. Куперштейн, канд. техн. наук, доц.

ГІБРИДНА БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ ВУЗЛІВ ПІРИНГОВОЇ МЕРЕЖІ

Розроблено метод гібридної багатофакторної автентифікації вузлів у пірінговій мережі. Метод включає автентифікацію як початкових вузлів, так і вторинних (що приєднуються до наявної мережі). Кожен вузол повинен спочатку здійснити автентифікацію сервером, в результаті якої отримає токен доступу до сервера, комунікативний токен (необхідний для здійснення комунікації з вузлом), а також службовий токен (для обміну службовими даними з іншими вузлами). Далі вузол повинен бути автентифікований іншим вузлом. Для цього використовуються завчасно визначені ідентифікатори, метод доказу нульового знання та мережа довіри. Знаючи ідентифікатор іншого користувача вузол може бути автентифікованим після проходження верифікації методом доказу нульового знання у три етапи. Спочатку верифікується те, що вузол володіє знанням адреси сервера. Далі верифікується валідність токену за допомогою перевірки дати його видачі (при цьому бере участь сервер, який надає дату видачі по ідентифікатору). Останнім кроком є перевірка того, чи вузол може вірно зашифрувати певні дані. Для цього генерується псевдовипадкова послідовність чисел, яку повинен зашифрувати сервер, а також вузол. Ключ для шифрування відомий лише серверу та вузлу (при серверній автентифікації генерується ключ для кожного вузла). Якщо всі етапи верифікації успішні, то вузли обмінюються ідентифікаційними даними, а отже стають взаємно автентифікованими. За допомогою мережі довіри, якщо два вузли не є взаємно автентифікованими, але є автентифікованими третім вузлом, то вони можуть напряму обмінятись ідентифікаційними даними без проходження процесу верифікації за допомогою доказу нульового знання. Запропонований метод спрямований на підвищення рівня захищеності пірингових мереж. Важливим аспектом є можливість відсікання потенційно шкідливих вузлів перед їх фактичним приєднанням до мережі.

Ключові слова: *пірингова мережа, автентифікація, доказ нульового знання, ідентифікатор, мережа довіри, шифрування, токен доступу, комунікація, сервер.*

Вступ

Сьогодні люди активно використовують різні програми та сервіси для комунікації. У цьому контексті захист даних стає дедалі важливішим завданням у сучасному цифровому світі [1]. Зазвичай комунікаційні платформи є загальнодоступними та базуються на центральному сервері, який виступає основним вузлом у всій комунікації та зберігає всі дані. Однак, навіть при використанні різноманітних криптографічних алгоритмів та інших методів захисту, центральний сервер має ряд недоліків, особливо у випадках корпоративної комунікації, оскільки корпоративні дані є конфіденційними і не повинні потрапити до рук зловмисників.

Для забезпечення захисту корпоративних даних все частіше починають використовуватись пірингові мережеві технології, які спрямовані на забезпечення цілісності, доступності та конфіденційності [2]. Пірингові мережі (peer-to-peer – P2P) – це тип мереж, де учасники обмінюються даними без централізованого органу управління (сервера). Їх популярність зростає, але це також підсилює важливість питання кібербезпеки [3]. Одним із ключових завдань забезпечення конфіденційності є автентифікація вузлів у пірінговій мережі. Через напівдовірений характер P2P-мереж автентифікація є критично важливою для ідентифікації користувачів та, в подальшому, захищеного обміну даними. У децентралізованих мережах реалізація механізму автентифікації є досить складною через відсутність єдиного достовірного джерела інформації для підтвердження ідентичності користувача. Тому актуальним завданням є розробка методу автентифікації вузлів у пірінговій мережі, який забезпечить високий рівень захищеності.

Постановка проблеми

Основною проблемою піринговых мереж є те, що через їхню децентралізовану структуру захищеність не реалізовується так само, як у клієнт-серверній архітектурі. Захист піринговых мереж досягається за допомогою шифрування даних, автентифікації вузлів, обмеження доступу, системи моніторингу трафіку, виявлення та запобігання шкідливій активності тощо [4].

Автентифікація вузлів є першим етапом для забезпечення безпечної комунікації вузлів піринговой мережі (рис. 1) [5]. Щоб два вузли могли взаємодіяти, спочатку кожен з них має пройти процес автентифікації. Після цього вони повинні успішно обмінятися ідентифікаційними даними. Лише після того вузли можуть встановити з'єднання і розпочати обмін даними.

Рис. 1. Необхідні кроки перед початком комунікації

У піринговых мережах існує три підходи до автентифікації користувачів:

1. Завчасно визначені ідентифікатори, які видаються в ручному режимі або можуть бути надіслані стороннім програмним забезпеченням [6]. При цьому ручний режим є доволі надійним, проте складним у використанні. Надсилання стороннім програмним забезпеченням є доволі зручним, проте менш захищеним, оскільки дані можуть потрапити у руки зловмисника.
2. Мережа довіри (web of trust) є одним із способів вирішити проблему відсутності довіреного центрального органу [7]. Підхід базується на принципі транзитивності, а саме, якщо вузол A довіряє вузлу B, а вузол B довіряє вузлу C, то вузол A може довіряти вузлу C. Відповідно далі вузли A та C можуть далі здійснювати комунікацію.
3. Доказ нульового знання (ДНЗ), суть якого полягає у доведенні однією стороною іншій, що твердження (зазвичай математичне) є істинним, при цьому будь-яка секретна інформація окрім істинності твердження не розповсюджується [8]. Обчислення в системах ДНЗ можуть виконуватися шляхом створення випадкових чисел як вхідних даних. Концепція, що лежить в основі доказу нульового знання, полягає у перевірці верифікатором V того, що вузол A знайомий із секретом S, при цьому сам секрет не передається верифікатору V. Тобто, верифікатор не знає ніякої інформації про невідоме, але може підтвердити, що вузол володіє цим секретом. Верифікатор ставить вузлу різні запитання, і у випадку всіх вірних відповідей, може стверджувати, що верифікація успішна. Проте розробка ефективних ДНЗ-протоколів є завданням, що вимагає великої уваги до безпеки та врахування потенційних атак [9].

Виходячи із вищеописаних переваг та недоліків кожного з підходів, пропонується використати гібридну багатофакторну автентифікацію. Це пов'язано з тим, що однофакторної автентифікації у піринговых мережах недостатньо. Використання лише центрального серверу не забезпечує достатній рівень автономності, безпеки та відмовостійкості, адже централізована система є вразливою до різних атак, наприклад методом «грубої сили» чи за допомогою атаки «маскарад». В результаті зловмисник може отримати ідентифікаційні дані вузлів [10]. Використання лише завчасно визначених ідентифікаторів неможливе за рахунок великої складності масштабування мережі, адже за умови невикористання сторонніх каналів зв'язку необхідна фізична присутність користувачів. Мережа довіри є механізмом, який працює лише у поєднанні з іншими методами, оскільки мають бути попередньо автентифіковані іншими методами вузли, що в

свою чергу зможуть бути взаємно автентифіковані за принципом мережі довіри.

Отже, вузлу пірингової мережі необхідно здійснити гібридну багатофакторну автентифікацію, що включає в себе використання центрального сервера для першого етапу та інший вузол для другого.

Результати дослідження

Нехай є учасник, що бажає доєднатись до мережі (стати вузлом мережі), що може бути двох типів: початковий P_n (той, що стане першим вузлом нової мережі) та вторинний P_k (той, що доєднається до наявної мережі).

Розглянемо процес автентифікації початкового вузла P_n.

Новий учасник P_n, який хоче приєднатися до певної мережі A, повинен спочатку пройти процедуру автентифікації F за допомогою клієнт-серверної частини мережі. Цей процес включає в себе перевірку та підтвердження ідентичності нового учасника. Після успішної автентифікації через сервер

$$RA = F(P_n), \quad (1)$$

де RA – результат автентифікції, $F(P_n)$ – функція автентифікації; учасник отримує унікальний ідентифікатор Id та набір ключів $K = \{k_1, k_2, k_s\}$, де k_1 – симетричний ключ для шифрування службових даних, а k_2 – пара ключів (публічний та приватний), що буде використовуватись для шифрування ідентифікаційних даних, k_s – ключ для шифрування даних, якими вузол обмінюється з сервером. Додатково, учасник отримує набір токенів $T = \{t_a, t_c, t_s\}$, які передбачені політикою безпеки. Токени є формату JWT (Json Web Token) [11]. Кожен такий токен містить корисне навантаження (payload), в яке можна додати необхідні для вузлів дані. Таким чином, сформовано корисне навантаження токенів (рис. 2 – рис. 4).


```
{
"createdAt": 1713123901470,
"id": "65959cd4-d8f1-4523-895a-2e3137e87425",
"type": "serverAccess"
}
```


Рис. 2. JWT payload токену доступу


```
{
"createdAt": 1713124968688,
"id": "65959cd4-d8f1-4523-895a-2e3137e87425",
"type": "communication",
"trustLevelCount": 14
}
```


Рис. 3. JWT payload токену доступу


```
{
"createdAt": 1713125070193,
"id": "65959cd4-d8f1-4523-895a-2e3137e87425",
"type": "service"
}
```


Рис. 4. JWT payload токену доступу

За допомогою першого t_a вузли матимуть змогу здійснити запити до сервера для отримання певної службової інформації. За допомогою другого токену t_c вузли матимуть змогу надсилати дані іншим вузлам (а ті в свою чергу мають їх валідувати перш ніж відповідати на

запит). За допомогою третього токена t_s вузли можуть здійснювати обмін службовими даними. Під час видачі токена доступу t_a, сервер реєструє дату та час його видачі, що також зашифровано в самому токені. Ці дані є важливим елементом для визначення часового контексту та можуть бути використані для подальшого контролю доступу та здійснення верифікації вузлів у мережі. Таким чином, результат функції автентифікації RA можна представити наступним чином:

$$RA = \{Id, K, T\}. \quad (2)$$

Розглянемо процес автентифікації вторинного вузла:

1. Перший етап аналогічний як для нового учасника, так і для вузла, який долучається до наявної мережі. У обох випадках учасник повинен пройти процедуру автентифікації за допомогою клієнт-серверної частини мережі для забезпечення безпеки та визначення ідентифікаторів та ключів для подальшої взаємодії в мережі.

2. Після успішного підтвердження сервером, учасник $b_j \in B$ може бути автентифікованим, знаючи ідентифікаційні дані іншого вузла $b_i \in B$, або ж, маючи лише ідентифікатор, бути автентифікованим після проходження верифікації вузлом b_j. Верифікація відбувається методом доказу нульового знання, тобто виконується деяка функція

$$ZNPR = ZNPF(b_j), \quad (3)$$

де $ZNPR$ – результат верифікації, $ZNPF$ – функція верифікації. Суб'єктом перевірки виступає токен доступу t_a вузла b_j. Відбувається обмін даними у форматі питання-відповідь, а саме (рис. 5):

a. Вузол b_i надсилає запит Q_1 до учасника b_j, щоб отримати у відповідь адресу сервера Res_1.

b. Учасник b_j надсилає відповідь Res_1.

$$Res_1 = Ans(Q_1), \quad (4)$$

де Ans – функція надання відповіді.

c. Вузол b_i порівнює її з тим, що відомо йому, а саме $Addr$. Якщо значення рівні

$$CHK_1 = (Res_1 \Leftrightarrow Addr), \quad (5)$$

де CHK_1 – результат перевірки, то верифікатор (вузол b_i) переходить до наступного запитання. В іншому випадку процес зупиняється, і учасник b_j додається у чорний список мережі, оскільки може бути зловмисним.

d. Вузол b_i надсилає запит Q_2 учаснику b_j, яка дата та час видачі токена dt_{t_a}. При цьому також вузол b_i надсилає запит Q_2' на сервер з метою отримання інформації про дату та час видачі токену dt'_{t_a} по певному ідентифікатору $dt^s_{t_a}$ (при цьому ні вузол, ні сервер не знають самого токена).

$$dt_{t_a} = Ans(Q_2), \quad (6)$$

$$dt'_{t_a} = Ans(Q_2'). \quad (7)$$

e. У випадку, якщо відповідь учасника b_j та сервера однакові

$$CHK_2 = (dt_{t_a} \Leftrightarrow dt'_{t_a}), \quad (8)$$

де CHK_2 – результат перевірки, то верифікатор переходить до наступного запитання. Якщо ні – процес зупиняється, і учасник b_j додається у чорний список мережі.

f. Вузол a_i генерує псевдовипадкову послідовність чисел NS і надсилає запит Q_3 учаснику b_j, щоб він зашифрував його своїм ключем з токена доступу. Очікується відповідь Res_3. Також такий самий запит Q_3' надсилається на сервер і очікується у відповідь зашифроване значення з сервера Res_3':

$$Res_3 = Ans(Q_3), \quad (9)$$

$$Res_3' = Ans(Q_3') \quad (10)$$

g. У випадку, якщо відповідь сервера така ж, що й учасника b_j, то етап верифікації є успішно завершеним. Інакше – учасник b_j додається до чорного списку мережі, оскільки може бути зловмисним. Функція перевірки представлена наступним чином:

$$CHK_3 = (Res_3 = Res_3'), \tag{11}$$

де CHK_3 – результат перевірки.

$$ZNPR = \{CHK_1, CHK_2, CHK_3\}. \tag{12}$$

Таким чином усі $CHK_i \in CHK$, де CHK – множина результатів перевірки верифікатором учасника, повинні мати значення «істини», що означає успішну верифікацію. Після успішної верифікації вузлом a_i, учасник b_j стає автентифікованим вузлом мережі. Вузол b_i надсилає вузлу b_j усі необхідні дані для подальшої комунікації.

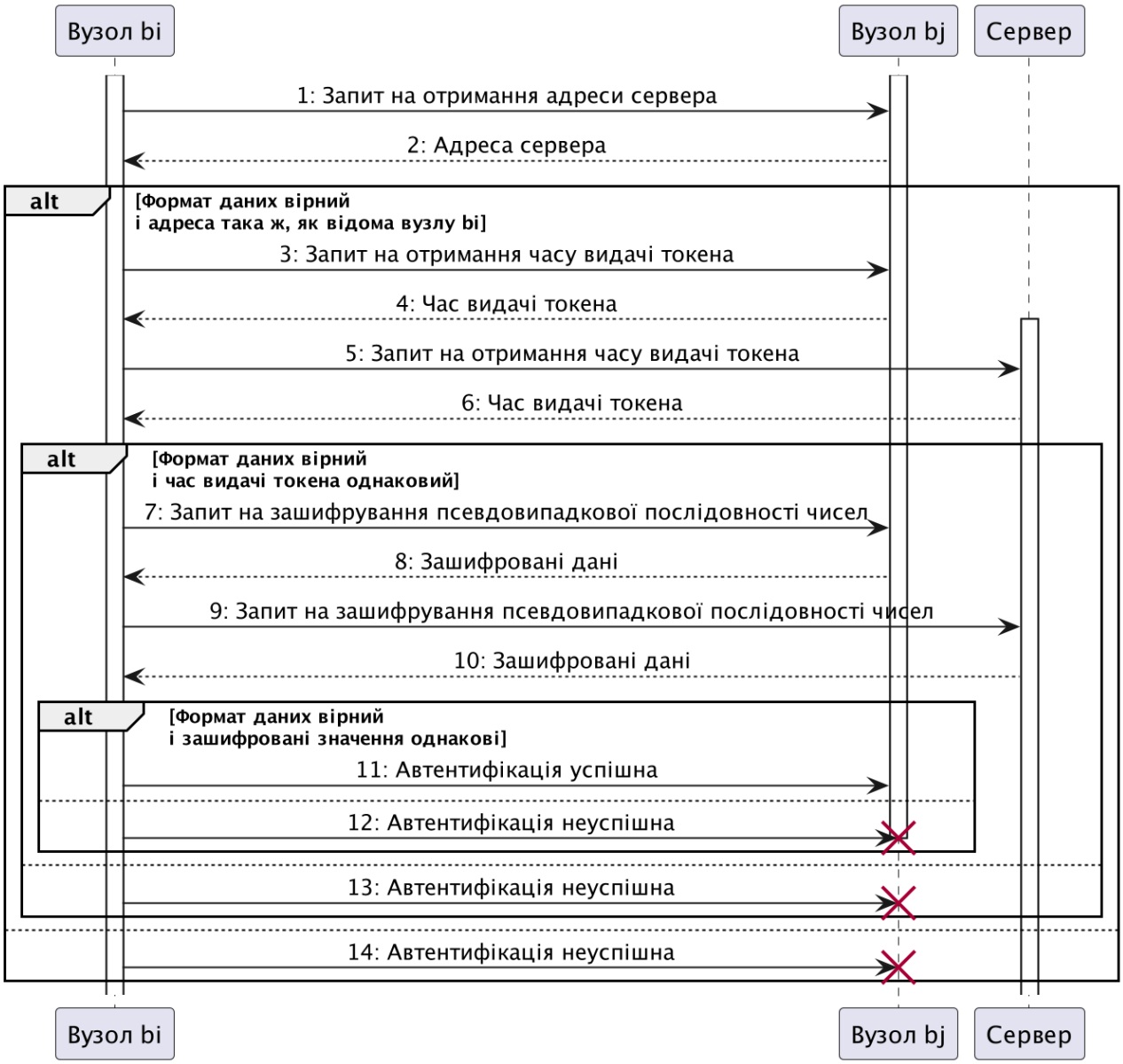

Рис. 5 – UML-діаграма процесу верифікації вузла

На основі методу мережі довіри, вузол b_j може здійснювати обмін даними з іншими вузлами мережі. Тобто якщо вузол b_i верифікував вузол b_j і він частиною мережі, а також вузол b_i здійснює комунікацію з певним вузол b_k, то за принципами мережі довіри, вузол b_j зможе встановити з'єднання з вузлом b_k без процесу проходження верифікації. Формально,

$(b_i \Rightarrow b_j), (b_i \Rightarrow b_k) \Rightarrow (b_j \Rightarrow b_k), i \neq j \neq k$. Таким чином, за принципом мережі довіри, вузол b_j має право отримати ідентифікаційні вузла b_k та мати змогу здійснювати з ним комунікацію.

Висновки

Розроблено метод автентифікації вузлів у пірінговій мережі, який представляє собою гібридний багатофакторний процес. Метод об'єднує в собі три основні методи автентифікації: завчасно визначені ідентифікатори, доказ нульового знання та мережу довіри. Додатково, сервер необхідний для здійснення першого етапу автентифікації перед тим, як буде здійснюватися автентифікація іншим вузлом. Також сервер використовується для кількох кроків верифікації методом ДНЗ.

Розроблений метод можна використати для підвищення захищеності пірингових мереж. Важливим аспектом є можливість відсікання потенційно шкідливих вузлів перед їх фактичним приєднанням до мережі. Процес відсікання реалізований на кількох етапах, що забезпечує високу надійність та ефективність у процесі автентифікації.

СПИСОК ЛІТЕРАТУРИ

1. Куперштейн Л. М. Аналіз тенденцій розвитку пірингових мереж / Л. М. Куперштейн, М. Д. Кренцін // Вісник Хмельницького національного університету. – 2021.– № 4. – С. 25 – 29.
2. A privacy data leakage prevention method in P2P networks [Електронний ресурс] / Cheol-Joo Chae // Peer-to-Peer Networking and Applications. – 2015. – Т. 9, № 3. – С. 508 – 519. – Режим доступу : https://doi.org/10.1007/s12083-015-0371-x.
3. Аналіз проблем безпеки пірингових мереж / Л. М. Куперштейн, М. Д. Кренцін, А. В. Дудатьєв [та ін.] // Інформаційні технології та комп'ютерна інженерія. – 2022. – № 2. – С. 5 – 14.
4. Qureshi H. P2P Networking [Electronic resource] / Haseeb Qureshi // NAKAMOTO. – Access mode : https://nakamoto.com/p2p-networking.
5. Yik L. Z. A Systematic Literature Review on Solutions of Mutation Testing Problems [Електронний ресурс] / Loh Zheung Yik, Wan Mohd Nasir bin Wan Kadir, Noraini binti Ibrahim // 2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS), Penang, Malaysia, 25 – 27 серп. 2023 р. – Режим доступу : https://doi.org/10.1109/icsecs58457.2023.10256324.
6. Identifier | Encyclopedia of Computer Science [Electronic resource] // DL Books. – Access mode : https://dl.acm.org/doi/abs/10.5555/1074100.1074468.
7. Anonymous and Distributed Authentication for Peer-to-Peer Networks [Електронний ресурс] / Pasan Tennakoon // Journal of Computer Science. – 2023. – Т. 19, № 1. – С. 1 – 10. – Режим доступу : https://doi.org/10.3844/jcssp.2023.1.10.
8. A Resilient Group Session Key Authentication Methodology for Secured Peer to Peer Networks using Zero Knowledge Protocol [Електронний ресурс]. – Режим доступу : https://doi.org/10.1016/j.ijleo.2022.170345.
9. Establishing Trust using Zero Knowledge Succinct Proof in Peer-to-peer Data Transfer [Електронний ресурс] / Sai Kiran Deversetti // Proceedings of 36th International Conference on Computer Applications in Industry and Engineering. – Режим доступу: https://doi.org/10.29007/jqw8.
10. Magnusson A. 11 Common Authentication Vulnerabilities You Need to Know | StrongDM [Електронний ресурс] / Andrew Magnusson // StrongDM: Your Partner in Zero Trust Privileged Access. – Режим доступу : https://www.strongdm.com/blog/authentication-vulnerabilities.
11. JWT.IO [Електронний ресурс] // JSON Web Tokens - jwt.io. – Режим доступу : https://jwt.io/.

Стаття надійшла до редакції 23.06.2024.
Стаття пройшла рецензування 27.06.2024.

Кренцін Михайло Дмитрович – аспірант кафедри захисту інформації.
Вінницький національний технічний університет.

Куперштейн Леонід Михайлович – канд. техн. наук, доцент кафедри захисту інформації.
Вінницький національний аграрний університет.