Метод Гібридної Багатофакторної Аутентифікації Вузлів у Піринговій Мережі

Михайло Кренцін
кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
mishatron98@gmail.com

Леонід Куперштейн
кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
kupershtein.lm@gmail.com

The Method of Hybrid Multifactor Authentication of Nodes in a Peer-To-Peer Network

Mykhailo Krentsin
dept. of information protection
Vinnytsia national technical university
Vinnytsia, Ukraine
mishatron98@gmail.com

Leonid Kupershtein
dept. of information protection
Vinnytsia national technical university
Vinnytsia, Ukraine
kupershtein.lm@gmail.com

***Анотація*—Запропоновано метод гібридної багатофакторної аутентифікації вузлів у піринговій мережі. Метод передбачає аутентифікацію як нового вузла, так і відомого. Передбачає використання завчасно визначених ідентифікаторів, доказу нульового знання та мережу довіри. Розроблений метод використовується для підвищення захищеності пірингових мереж**

***Abstract*—A method of hybrid multifactor authentication of nodes in a peer-to-peer network is proposed. The method provides authentication of both a new node and a known one. It includes the use of pre-defined identifiers, zero-knowledge proof, and a network of trust. The developed method is used to increase the security of peering networks**

Ключові слова—пірингова мережа; аутентифікація; мережа довіри; доказ нульового знання; токен доступу; шифрування; сервер; комунікація; ідентифікатор

Keywords—peer-to-peer network; authentication; web of trust; zero-knowledge proof; access token; encryption; server; communication; identidier

I. Вступ

На сьогоднішній день люди використовують різноманітні програми та сервіси для здійснення комунікації між собою. Водночас із цим захист даних стає все більш критичним завданням у сучасному цифровому світі [1]. Зазвичай платформи для комунікації є загальнодоступними та передбачають використання центрального сервера, який є основною ланкою у всій комунікації та зберігає усі дані. Проте, навіть з урахуванням того, що використовуються різноманітні криптографічні алгоритми та інші методи захисту даних, використання центрального сервера має ряд недоліків, особливо, коли здійснюється корпоративна комунікація, адже корпоративні дані є конфіденційними і не повинні потрапити у руки зловмисника.

Для забезпечення конфіденційності корпоративних даних використовуються пірингові мережі (P2P), що спрямовані на забезпечення цілісності, доступності та конфіденційності обмінюваних даних. Пірингові мережі – це вид мереж, де учасники обмінюються даними без централізованого сервера [2]. Вони стають все більш популярними, але й роблять питання конфіденційності ще більш гострим. Першочерговим постає питання аутентифікації вузлів у піринговій мережі. Через напівдовірений характер мереж P2P аутентифікація відіграє важливу роль в ідентифікації користувача в мережі, автентичності та цілісності обміну інформацією. У децентралізованих мережах реалізувати механізм аутентифікації досить складно, оскільки немає єдиного достовірного джерела інформації, що підтвердить ідентичність користувача. Тому актуальним є розробка методу аутентифікації вузлів у піринговій мережі, що буде забезпечувати високу надійність та ефективність процесу.

II. Результати дослідження

Аутентифікація є найважливішим аспектом безпеки пірингових мереж. Загалом, аутентифікація – це процедура встановлення належності користувачеві пред’явленого ним ідентифікатора [3]. Аутентифікація є однофакторна та багатофакторна (де до уваги береться два чи більше факторів).

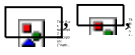
У пірингових мережах існує 3 підходи здійснення аутентифікації користувачів:

- Завчасно визначені ідентифікатори. Вони видаються в ручному режимі, або можуть бути надіслані стороннім програмним забезпеченням (ПЗ). Ручний режим є досить надійним, проте неавтоматизований та складний у використанні [4]. Надсилання ідентифікатора іншому вузлу зв допомогою стороннього ПЗ є доволі зручним, але менш надійним способом, оскільки ідентифікаційні дані можуть потрапити у руки зловмисника.

- Мережа довіри (web of trust). Вперше ця концепція була представлена Філом Ціммерманом у 1992 році [5]. Мережа довіри дозволяє вирішити проблему відсутності довіреного центрального органу. Реалізується це за допомогою принципу транзитивності. Наприклад, якщо вузол $a_i \in A$ довіряє вузлу $b_j \in B$, а вузол $b_j \in B$ довіряє вузлу $c_k \in C$, то вузол $a_i \in A$ може довіряти вузлу $c_k \in C$, а отже, встановлювати з'єднання для подальшої комунікації.

- Доказ нульового знання (ДНЗ). Полягає в тому, що одна сторона доводить іншій, що твердження є істинним, але без розкриття будь-якої іншої інформації, окрім достовірності твердження. Концепція, що лежить в основі ДНЗ, передбачає перевірку верифікатором V, що вузол $a_i \in A$ знайомий із секретом, при цьому сам секрет не передається верифікатору V [6]. Перевірка здійснюється завдяки постановки різних запитань та перевірки відповідей.

Для зменшення ризику несанкціонованого доступу та підвищення загального рівня безпеки мережі було прийнято рішення об'єднати вищеописані методи аутентифікації. Це пов'язано з тим, що односторонньої аутентифікації у пірингових мережах недостатньо, оскільки це є вразливістю до атак «Людина посередині» [7]. Використання лише центрального серверу є не забезпечує достатній рівень безпеки та відмовостійкості, оскільки може бути зламаний (наприклад методом «Brute-force» або «Грубої сили» чи за допомогою атаки «Маскарад»), і тоді в руки зловмисника потраплять ідентифікаційні дані вузлів [8]. Використання лише завчасно визначених ідентифікаторів неможливе за рахунок великої складності масштабування мережі, оскільки необхідна фізична присутність користувачів (за умови невикористання сторонніх каналів зв'язку для поширення ідентифікаційних даних). Мережа довіри є механізмом, який працює лише у поєднанні з іншими методами, оскільки мають бути попередньо аутентифіковані іншими методами вузли, які потім можуть бути взаємно аутентифіковані за принципом мережі довіри. Використання доказу нульового знання є досить ефективним способом аутентифікації вузлів, проте необхідно мати якийсь секрет для верифікації, і для надійності цей секрет повинен бути згенерований третьою стороною. Таким чином, вузлу пірингової мережі необхідно здійснити гібридну багатофакторну аутентифікацію, що включає в себе використання центрального сервера для першого етапу та інший вузол для другого. Учасник, що хоче доєднатись до мережі може бути як новим (буде першим учасником підмережі), так і відомим (той, що встановлює з'єднання з існуючою підмережею).

1. Новий або відомий учасник $a_i \in A$, який хоче приєднатися до мережі A, повинен першочергово пройти процедуру аутентифікації F за допомогою клієнт-серверної частини гібридної пірингової мережі. Цей процес передбачає перевірку та підтвердження ідентичності нового учасника. Після успішної аутентифікації $F(p)$ через сервер, учасник отримує унікальний ідентифікатор Id та набір ключів $K = \{k_1, k_2\}$, де k_1 – симетричний ключ для шифрування службових даних, а k_2 – пара ключів (публічний та приватний), що буде використаний для наскрізного шифрування при комунікації двох вузлів. Далі учасник отримує токен доступу до серверу (access token). Сервер реєструє дату час видачі токена. Це саме значення і зашифроване в самому токені. Також токен містить симетричний ключ, який використовується для шифрування обмінюваних з сервером даних. Вищеописані дані є важливою складовою для визначення часового контексту та будуть використані для подальшої аутентифікації.
2. Якщо вузол не є новим, то після успішної серверної аутентифікації, вузол $b_j \in B$ обмінюється ідентифікаційними даними з вузлом $a_i \in A$ і очікує результату верифікації, що відбувається за допомогою доказу нульового знання. Суб'єктом перевірки виступає токен доступу вузла $b_j \in B$. Відбувається обмін даними у форматі питання-відповідь, а саме (рис. 1):
   a. Вузол a_i надсилає запит до учасника b_j, щоб отримати у відповідь адресу сервера. Учасник b_j надсилає відповідь. Вузол a_i порівнює її з тим, що відомо йому. Якщо значення рівні, то верифікатор (вузол a_i) переходить до наступного питання. В іншому випадку процес зупиняється, і учасник b_j додається у чорний список підмережі, оскільки може бути зловмисним. Таким чином $Res_1 = Ans(Q_1)$, де Res_1, Ans, Q_1 – результат, функція надання відповіді учасником та питання верифікатора відповідно.
   b. Вузол a_i надсилає запит учаснику  і очікує у відповідь дату та час видачі токена. Також вузол  надсилає запит на сервер аби отримати дані про дату та час видачі токену по певному ідентифікатору, а саме по ідентифікатору вузла  (при цьому ні вузол, ні сервер не знають самого токена, що й характерно для ДНЗ). Якщо відповідь учасника  та сервера однакові, верифікатор переходить до наступного запитання. В іншому випадку процес зупиняється, і учасник  додається у чорний список підмережі, оскільки може бути зловмисним. Таким чином  , де 

– результат, функція надання відповіді, питання та відповідь на запит до сервера відповідно.

с. Вузол генерує псевдовипадкову послідовність чисел і надсилає запит учаснику щоб він зашифрував його своїм ключем з токена. Також такий самий запит надсилається на сервер і очікується у відповідь зашифроване значення з сервера і від учасника. У випадку, якщо відповідь сервера така ж, що й учасника то етап верифікації є успішно завершеним. Інакше – учасник додається до чорного списку підмережі, оскільки може бути зловмисним. Таким чином , де ; ; – результат, функція надання відповіді, питання та відповідь на запит до сервера відповідно.

Отже, усі , де – множина результатів відповідей на питання верифікатора, повинні мати значення «істини», що означає успішну верифікацію. Далі вузол надсилає вузлу усю необхідну службову інформацію.

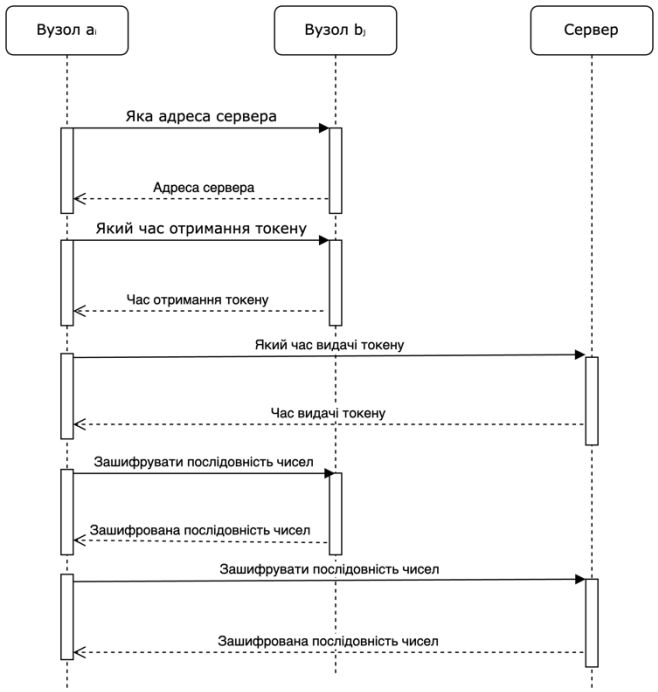


Рис. 1 – Діаграма послідовностей процесу верифікації вузла

На основі методу мережі довіри, вузол може здійснювати обмін даними з іншими вузлами підмережі. Оскільки вузол верифікував вузол і він є частиною підмережі, а також вузол здійснює комунікацію з певним вузлом то за принципами мережі довіри, вузол зможе встановити з'єднання з вузлом без процесу проходження верифікації (але знаючи ідентифікатор). Формально, . Таким чином, на основі принципу мережі довіри, вузол може здійснювати комунікацію з

Таким чином, розроблено метод гібридної багатофакторної аутентифікації вузлів у піринговій мережі. Метод об'єднує в собі три основні методи аутентифікації: завчасно визначені ідентифікатори, доказ нульового знання та мережу довіри

Висновки

Розроблено метод аутентифікації вузлів у децентралізованій мережі. Аутентифікація є гібридною багатофакторною, що поєднує у собі завчасно визначені ідентифікатори, доказ нульового знання та мережу довіри. Також передбачає використання сервера для першого етапу аутентифікації.

Розроблений метод використовується для підвищення захищеності пірингових мереж. Перевагою методу є можливість блокування потенційно зловмисних вузлів до їх приєднання до мережі. Усі кроки аутентифікації забезпечують її високу надійність та ефективність.

Література References

[1] Куперштейн Л.М, Кренцін М.Д. Аналіз тенденцій розвитку пірингових мереж. Вісник Хмельницького національного університету. – №4. – 2021. – С.25-29.

[2] Куперштейн Л.М, Кренцін М.Д., Дудатьєв А.В., Каплун В.А. Аналіз проблем безпеки пірингових мереж. Інформаційні технології та комп'ютерна інженерія. – №2. – 2022. – С.5-14.

[3] What Is Authentication? Definition and Methods | Microsoft Security. [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-authentication.

[4] P2P Networking. [Online]. Available: https://nakamoto.com/p2p-networking/.

[5] Anonymous and Distributed Authentication for Peer-to-Peer Networks [Online]. Available: https://eprint.iacr.org/2021/838.pdf

[6] A resilient group session key authentication methodology for secured peer to peer networks using zero knowledge protocol. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0030402622016035.

[7] How to perform authentication without central server in P2P? [Online]. Available: https://crypto.stackexchange.com/questions/12479/how-to-perform-authentication-without-central-server-in-p2p.

[8] 11 Common Authentication Vulnerabilities You Need to Know. [Online]. Available: https://www.strongdm.com/blog/authentication-vulnerabilities