УДК 004.021 DOI: 10.18372/2073-4751.73.17642

Макаренко О.І., к.т.н.,
Охріменко Т.О., к.т.н.,
orcid.org/0000-0001-9036-6556,
Бредніков А.В.

НОВИЙ ПІДХІД ГЕНЕРАЦІЇ МНЕМОНІЧНИХ ФРАЗ НА ОСНОВІ МЕДІА ФАЙЛІВ

Національний авіаційний університет

t.okhrimenko@nau.edu.ua

Вступ

Безпека мнемонічних фраз-паролів [1] значною мірою залежить від міцності початкової фрази, яка часто генерується за допомогою генератора псевдовипадкових чисел (PRNG) [2]. У цій статті запропоновано новий підхід до генерації мнемонічних парольних фраз із використанням медіафайлів як джерела випадковості.

Розроблений підхід базується на ідеї, що мультимедійні файли, такі як зображення чи аудіофайли, мають достатню ентропію [3], яку можна використовувати для генерування надійних початкових фраз.

Оцінюється безпека запропонованого підходу, порівнюючи згенеровані вихідні фрази з тими, які генеруються за допомогою стандартного PRNG. Запропонований підхід генерує початкові фрази з достатньою ентропією, що робить їх стійкими до брутфорс-атак. Крім того, продемонстровано, що розроблений підхід універсальний, оскільки різні типи медіа-файлів можна використовувати для створення початкових фраз.

Загалом розроблений новий підхід до зберігання мнемонічних парольних фраз забезпечує значне покращення безпеки та простоти використання порівняно з традиційними підходами, що робить його альтернативою для захисту криптовалютних гаманців.

Мета

Метою роботи є пропозиція по вдосконаленню підходу до генерування та зберігання мнемонічних фраз, що покликана посилити безпеку криптовалютных гаманців.

Огляд існуючих рішень. Мнемонічна фраза

Мнемонічна фраза, також відома як seed фраза, – це послідовність слів, які використовуються для генерації закритих ключів гаманця криптовалюти. Ці фрази зазвичай складаються з 12-24 слів і генеруються випадковим чином, щоб забезпечити високий рівень безпеки.

Мнемонічні фрази були введені в BIP39 (Bitcoin Improvement Proposal 39) [4] як спосіб спростити процес резервного копіювання та відновлення гаманців криптовалюти. Стандарт BIP39 визначає процес генерації мнемонічної фрази та перетворення її на бінарне початкове число, яке можна використовувати для отримання ієрархічного детермінованого (HD) гаманця.

Використання мнемонічних фраз стало загальною рисою для багатьох криптовалют, включаючи Bitcoin та Ethereum, і широко підтримується рядом програмних забезпечень та апаратних пристроїв гаманців. Використання стандартизованих фраз і можливість легкого резервного копіювання та відновлення гаманців за допомогою мнемонічних фраз значно спростило процес керування та захисту криптовалют.

embody color cushion despair monster motor match
despair much hammer actor bunker clip flush review
middle such sight ocean shock spray also twelve analyst

Рис. 1. Приклад мнемонічної фрази на 24 слова

Гарячий гаманець

Гарячий гаманець – це тип цифрового гаманця, який підключено до Інтернету та дозволяє користувачам легко та

швидко зберігати, надсилати та отримувати криптовалютні активи. Гарячі гаманці, як правило, призначені для частого використання, і доступ до них зазвичай здійснюється через веб-браузер або мобільну програму [5].

Однак, оскільки вони підключені до Інтернету, гарячі гаманці більш уразливі до загроз безпеці. Гарячі гаманці вразливі до хакерських та інших онлайн-атак, які можуть призвести до втрати коштів [6].

Кастодіальні гарячі гаманці керуються сторонніми компаніями або службами, які зберігають приватні ключі від імені користувача, що може бути точкою централізації та становити ризик для конфіденційності користувачів. У цьому випадку криптовалютні активи користувача знаходяться у зберігача, який відповідає за безпеку та управління активами. Зазвичай користувач має обліковий запис у зберігача, який надає доступ до функціоналу гаманця [7].

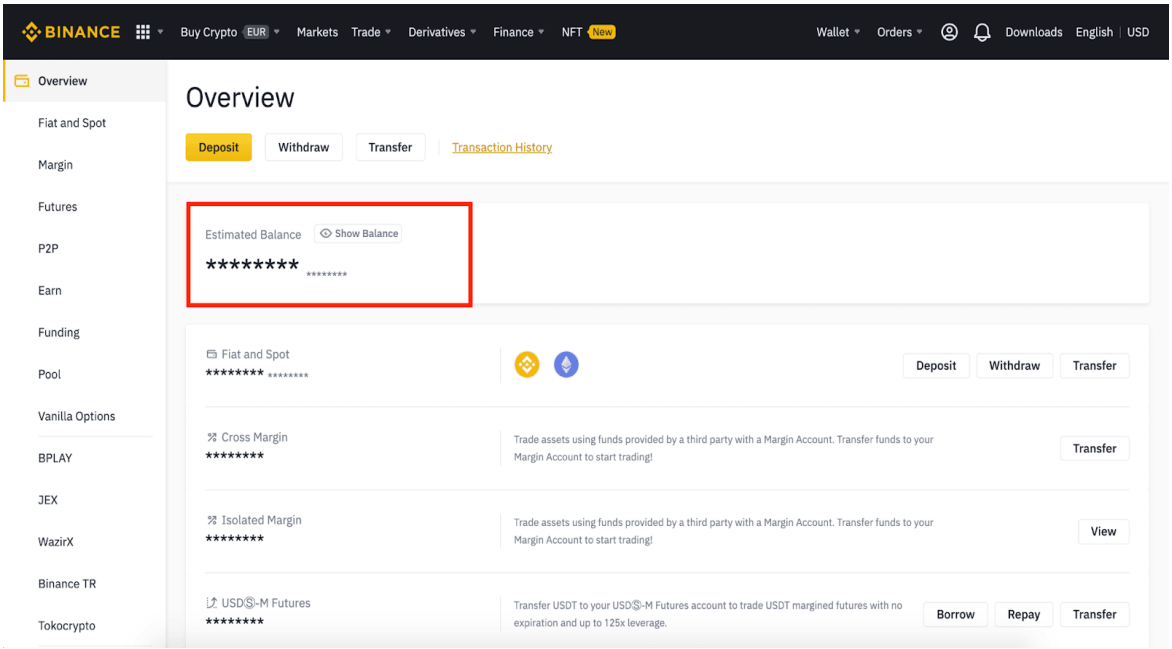

Рис. 2. Гарячий кастодіальний гаманець Binance

Гарячими некастодіальними гаманцями керує користувач, який відповідає за створення та зберігання власних закритих ключів. Користувач має повний контроль над своїми криптовалютними активами та може отримати доступ до свого гаманця за допомогою програмного додатка гаманця. Некастодіальні гарячі гаманці зазвичай пропонують більше контролю та безпеки, ніж кастодіальні гаманці, але вимагають більше технічних знань для керування.

Апаратний гаманець

Апаратний гаманець – це тип холодного криптовалютного гаманця, який не підключений до Інтернету, а отже, менш вразливий до злому та інших загроз безпеці [8]. Апаратні гаманці зазвичай мають вигляд невеликих пристроїв, що під'єднуються через провідні або безпровідні інтерфейси до пристрою з виходом до мережі інтернет. Апаратний гаманець лише зберігає мнемонічну фразу та підписує транзакції приватним ключем. Сам процес анонсу транзакції до блокчейну виконується пристроєм з виходом до мережі інтернет окремо. Оскільки апаратні гаманці не підключені до Інтернету, вони вважаються більш безпечними, ніж гарячі гаманці, які підключені до Інтернету і, отже, більш уразливі до онлайн-атак. Апаратні гаманці зазвичай використовуються для довгострокового зберігання криптова-люти, і зазвичай вони не так легко доступні, як гарячі гаманці.

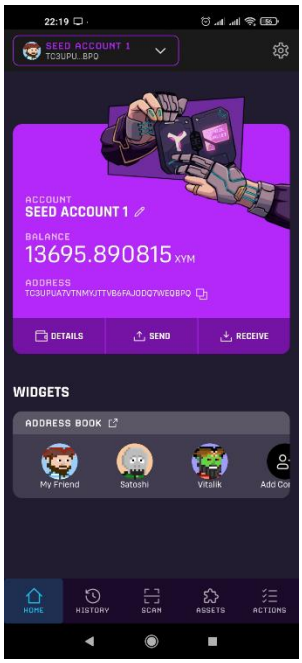

Рис. 3. Гарячий некастодіальний гаманець Symbol Mobile Wallet

Рис. 4. Апаратний гаманець Ledger Nano X

Хоча апаратні гаманці забезпечують підвищену безпеку для зберігання криптовалюти, вони можуть бути складнішими у використанні та потребують ретельного керування, щоб забезпечити безпеку та доступність коштів, що зберігаються в них. Також апаратні гаманці мають наступні недоліки:

1. Фізична втрата або пошкодження: оскільки апаратні гаманці є фізичними пристроями, вони вразливі до фізичної втрати або пошкодження, що може призвести до втрати доступу до збереженої криптовалюти.

2. Сумісність пристроїв: апаратні гаманці можуть бути несумісними з усіма типами операційних систем або пристроїв, що може обмежити їх корисність і доступність.

3. Атаки на ланцюг поставок: існує ризик того, що апаратний гаманець може бути скомпрометований під час виробничого процесу, дозволяючи зловмисникам отримати доступ до збереженої криптовалюти.

4. Помилка користувача: користувачі можуть випадково втратити або пошкодити свій апаратний гаманець, забути свої коди доступу або не створити резервну копію початкових фраз, що призведе до втрати доступу до їхньої криптовалюти.

5. Обмежене сховище: апаратні гаманці мають обмежений обсяг сховища, якого може бути недостатньо для деяких користувачів, які зберігають велику кількість валют.

6. Хоча апаратні гаманці зазвичай вважаються безпечними, завжди існує ймовірність невиявлених уразливостей, якими можуть скористатися зловмисники.

Паперовий гаманець

Паперовий гаманець – це тип холодного гаманця, який використовується для зберігання криптовалюти в автономному режимі [9]. Він передбачає запис мнемонічної фрази гаманця криптовалюти на аркуші паперу, який потім можна безпечно зберігати у фізичному місці. Оскільки паперові гаманці не підключені до Інтернету, вони не вразливі до злому та інших загроз онлайн-безпеці. Однак вони мають певні ризики та обмеження. Одним із основних ризиків, пов'язаних із паперовими гаманцями, є можливість фізичного пошкодження або втрати, що може призвести до втрати доступу до збереженої криптовалюти. Крім того, паперові гаманці можуть бути вразливими до крадіжки, оскільки будь-хто, хто отримує доступ до паперу, потенційно може використовувати

збережену мнемонічну фразу для доступу до пов'язаної криптовалюти.

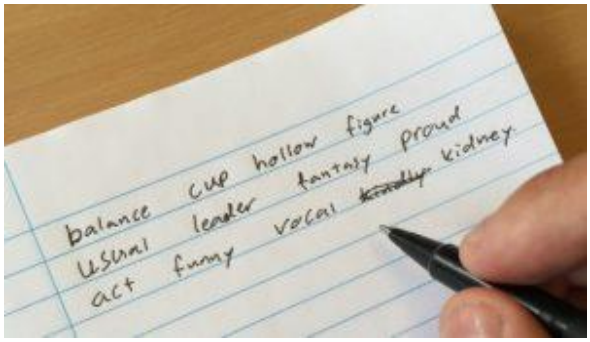

Рис. 5. Паперовий гаманець

Хоча апаратні гаманці зазвичай вважаються безпечними, вони все одно можуть бути вразливими до фізичного пошкодження або втрати. Якщо апаратний гаманець втрачено, викрадено або пошкоджено, що неможливо відновити, єдиний спосіб відновити доступ до криптовалюти, що зберігається в ньому – це використання резервної копії мнемонічної фрази. Резервне копіювання мнемоніки на папері забезпечує додатковий рівень захисту від втрати доступу до гаманця криптовалюти. Зберігаючи фізичну копію вихідної фрази в надійному місці, користувачі можуть бути впевнені, що вони зможуть відновити доступ до своїх коштів навіть у разі апаратної несправності, втрати або крадіжки. Аналогічно з гарячими гаманцями, доступ до яких може бути втрачено. Одночасно зі збільшенням безпеки доступу до гаманця, як гарячі, так і апаратні гаманці наслідують недоліки паперового гаманця в контексті компрометації мнемонічної фрази.

Генерація немонічної фрази із медіа файлу

Зазвичай гарячі та апаратні гаманці генерують мнемонічну фразу за допомогою комбінації випадковості та попередньо визначеного алгоритму. Процес призначений для того, щоб результуюча мнемонічна фраза була унікальною та непередбачуваною. Проте надійність згенерованої фрази залежить лише від реалізації процесу генерації розробниками гаманця. Також безпека криптовалютних активів залежить від того як саме зберігається мнемонічна фраза. Існуючі популярні методи зберігання фрази мають певні недоліки.

Пропонується розглянути новий підхід у генерації мнемонічної фрази. В якості джерела випадковості використовується медіафайл. Виокремимо ключові моменти:

Медіафайл повинен бути якомога менш розповсюдженим. Зі збільшенням числа користувачів файлу, збільшується вірогідність повторної генерації мнемонічної фрази. Рекомендується використовувати файл, що був створений майбутнім власником мнемонічної фрази.

В алгоритмі генерації мнемонічної фрази повинні використовуватися лише байти корисних даних. Метадані та інші службові дані специфікації файлу не повинні бути залучені у роботу алгоритму, так як вони знижують рівень ентропії [10].

Додатково згенерована фраза повинна бути зашифрована паролем користувача. Таким чином унеможливлюється атака грубого перебору медіафайлів на предмет наявності балансів активів, згенерованих з них.

Медіафайл може зберігатись на пристрої з виходом до мережі інтернет та використовуватись гарячим гаманцем. Цей підхід є більш безпечним у порівнянні зі звичайним зберіганням послідовності із 12 чи 24 слів у пам'яті електронно вимірювальної машини, чи на клаптику паперу. Зазвичай цільовій атаці піддаються гарячі гаманці та їх сховище даних, а також текстові файли що можуть містити фразу. Натомість файл, що був використаний у створенні мнемонічної фрази, знайти буде складно, так як ним може бути будь який файл на машині.

Одним із ключових факторів, що впливають на безпеку мнемонічної фрази, є якість випадковості, яка використовується для її створення. Якість випадковості, яка використовується для створення мнемонічної фрази, має вирішальне значення, оскільки вона визначає ентропію фрази. Ентропія є мірою випадковості, а вища ентропія означає, що фраза є більш безпечною та важкою для вгадування або

підбору грубої сили. Мнемонічна фраза, сумісна з BIP39, складається з 12 або 24 слів, які відповідають 128 або 256 бітам ентропії відповідно. Чим вища ентропія, тим надійніша мнемонічна фраза. Однією з проблем випадковості мнемонічної фрази є використання слабких джерел ентропії. Слабкі джерела ентропії, такі як парольні фрази, створені генераторами псевдовипадкових чисел (PRNG), які не є криптографічно захищеними, можуть призвести до мнемонічної фрази з низькою ентропією. Фраза з низьким рівнем ентропії вразлива до атак грубої сили, коли зловмисник намагається вгадати фразу, пробуючи всі можливі комбінації слів. Іншою проблемою випадковості мнемонічної фрази є ризик зіткнень. Зіткнення відбувається, коли дві різні мнемонічні фрази генеруються з однієї ентропії. Це може статися, якщо ентропія не є справді випадковою або якщо алгоритм, використаний для створення фрази, має недоліки. Якщо виникає колізія, це може поставити під загрозу безпеку обох гаманців, які використовують ту саму фразу. Натомість медіафайл має кращу ентропію та практично позбавлений колізії [11]. Наприклад, навіть 2 зображення JPEG зроблених за допомогою DSLR камери у режимі серійної зйомки матимуть різну послідовність байтів, незважаючи на майже однакове зображення [10].

Висновки

У статті розглянуто різні типи криптовалютних гаманців, що відрізняються за доступом до мережі інтернет та типом зберігання мнемонічної фрази. Результати демонструють, що підхід зберігання мнемонічної фрази у медіафайлі забезпечує кращу безпеку порівняно з традиційними методами зберігання мнемонічної парольної фрази. Крім того, запропонований підхід також покращує простоту використання, полегшуючи користувачам доступ до своїх гаманців.

Загалом розроблений підхід до генерації мнемонічних фраз-паролів за допомогою медіа-файлів забезпечує покращену безпеку порівняно зі стандартними підходами на основі PRNG, а також забезпечує універсальне та просте у використанні рішення для захисту гаманців криптовалюти.

Література

1. Wuille, P.: BIP32: Hierarchical Deterministic Wallets, February 2012. URL: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki.

2. Jasem F., Ali S., Awad A. Enhancement of digital signature algorithm in bitcoin wallet. Bulletin of Electrical Engineering and Informatics. – 2021. – Vol. 10. – P. 449-457.

3. Xuan G., Li X., Shi Y.-Q. Minimum entropy and histogram-pair based JPEG image reversible data hiding. Journal of information security and applications. – 2019. – Vol. 45. – P. 1-9.

4. *Palatinus M., Rusnak P., Voisine A., Bowe S.* Mnemonic code for generating deterministic keys, 2013. URL: https://github.com/bitcoin/bips/blob/master/bip-0039.

5. Hot and Cold Wallets. Ripple online documentation. URL: https: //ripple.com/build/gateway-guide/#hot-and-cold-wallets.

6. Jarecki S., Kiayias A., Krawczyk H., Xu J. Highly Efficient and Composable Password-Protected Secret Sharing (Or: How to Protect Your Bitcoin Wallet Online). 1st IEEE European Symposium on Security and Privacy, EuroS&P, 2016. URL: https://eprint.iacr.org/2016/144.

7. Chalkias K., Panagiotis Ch., Ji Y. Broken Proofs of Solvency in Blockchain Custodial Wallets and Exchanges. Workshop on Coordination of Decentralized Finance (CoDecFin) - FC 2022. – 2022. URL: https://eprint.iacr.org/2022/043.

8. *Hussain, S. Hasan, T. B. Sivakumar, and Alex Khang.* Cryptocurrency methodologies and techniques. The Data-Driven Blockchain Ecosystem. – CRC Press, 2022. – P. 21-29.

9. *Suratkar S., Shirole M., Bhirud S.* Cryptocurrency wallet: A review. 2020 4th international conference on computer, communication and signal processing (ICCCSP). – IEEE, 2020. – P. 1-7.

10. *Fridrich, J., Pevný T., Kodovský J.* Statistically undetectable jpeg steganography:

dead ends challenges, and opportunities. Proceedings of the 9th workshop on Multimedia & security. – 2007. – 11 p.

11. Sudharsanan S. Shared key encryption of JPEG color images. IEEE Transactions on Consumer Electronics. – 2005. – Vol. 51. – P. 1204-1211.

Макаренко О.І., Охріменко Т.О., Бредніков А.В.

НОВИЙ ПІДХІД ГЕНЕРАЦІЇ МНЕМОНІЧНИХ ФРАЗ НА ОСНОВІ МЕДІА ФАЙЛІВ

Мнемонічні парольні фрази стали популярним методом захисту криптовалютних гаманців завдяки простоті їх використання та можливості відновлення гаманців у разі втрати фізичних носіїв. Проте безпека мнемонічних фраз-паролів залежить від надійності початкової фрази та заходів безпеки, які використовуються для її зберігання та захисту. У цьому дослідженні оцінюється безпека зберігання мнемонічних парольних фраз і оцінюємо ризики, пов'язані з різними методами зберігання. Виявлено недоліки пов'язані з різними типами криптовалютних гаманців, зокрема, ймовірність витоку даних і хакерських атак, вразливості до фізичної крадіжки та пошкодження. Було запропоновано новий підхід у створенні та зберіганні мнемонічної фрази за допомогою медіа файлів. Отримані результати дають змогу зробити висновок, що запропонований підхід є більш безпечний за наявні методи зберігання мнемонічної фрази.

***Ключові слова**: детермінований гаманець, seed phrase, mnemonic, crypto wallet.*

Makarenko O.I., Okhrimenko T.O., Brednikov A.V.

A NEW APPROACH TO GENERATION OF MNEMONIC PHRASES BASED ON MEDIA FILES

Memorable passphrases have become a popular method of protecting cryptocurrency wallets due to their ease of use and the ability to restore wallets in case of loss of physical media. However, the security of mnemonic passphrases depends on the reliability of the seed phrase and the security measures used to store and protect it. This study evaluates the security of storing memorable passphrases and assesses the risks associated with other storage methods. Disadvantages associated with various types of cryptocurrency wallets have been identified, including the potential for data leakage and hacking attacks, vulnerability to physical theft and damage. A new approach was proposed in creating and storing a memorable phrase using media files. The obtained results make it possible to conclude that the proposed approach is more secure than the existing methods of preserving the ymonic phrase.

***Keywords**: deterministic wallet, initial phrase, mnemonic, crypto-wallet.*