УДК 004.056.53

АВТЕНТИФІКАЦІЯ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ БЛОКЧЕЙН

А. С. Карпець[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

У даній роботі наводиться новий спосіб проведення багатофакторної автентифікації користувача за допомогою технології блокчейн.

Ключові слова: багатофакторна автентифікація, блокчейн

Вступ

У захищених інформаційних системах будь-який суб'єкт доступу, перед початком роботи в системі, повинен пройти процедури ідентифікації, автентифікації та авторизації. Термін «автентифікація» означає процедуру перевірки та доведення справжності суб'єкта, який намагається отримати доступ до деякої захищеної системи, тому проходження автентифікації запобігає доступу небажаних осіб та забезпечує вхід легальних користувачів.

В наш час використання лише статичного пароля вже не є безпечним з точки зору надійності збереження та конфіденційності приватних даних. Тому багато популярних онлайн сервісів, банківських та хмарних систем пропонують своїм користувачам застосовувати у якості другого фактора автентифікації технологію одноразового паролю (англ. – «one-time-password», OTP). При цьому найбільш популярними способами доставки кодів автентифікації є надсилання їх за допомогою SMS-повідомлень або через мобільний додаток Google Authenticator.

Проте для даних засобів неодноразово були виявлені недоліки з точки зору безпеки їх використання [1, 2], тому в даній роботі буде запропоновано та проаналізовано новий підхід до проведення автентифікації за допомогою технології блокчейн.

1. Багатофакторна автентифікація

1.1. Схема багатофакторної автентифікації

Інформація, яку суб'єкт доступу надає системі для проходження автентифікації, називається фактором автентифікації. Загальноприйнята схема базується на трьох факторах:

- фактор знання (дещо, що знає суб'єкт) – таємні знання, якими може володіти лише авторизований суб'єкт, наприклад, пароль або PIN;
- фактор володіння (дещо, що суб'єкт має) – володіння суб'єктом деяким неповторним предметом, в який зберігаються дані для автентифікації;
- біометричний фактор (деяка біологічна особливість суб'єкта) – біометричні дані, такі, як сітківка ока, відбиток пальця, зразок рукописного чи клавіатурного почерку тощо.

Наведені вище фактори є основними і, як правило, вони найбільш розповсюджені в існуючих системах автентифікації, проте, часто в якості фактору використовується також фактор розташування (певне місцерозташування суб'єкта) – при проходженні автентифікації реєструється місцеположення та перевіряється, чи є воно типовим для даного суб'єкта. Також розповсюдженим є соціальний фактор – підтвердження автентичності суб'єкта за допомогою третьої сторони, а саме за допомогою попередньо обраних та завірених користувачем довірених осіб, які можуть підтвердити його достовірність при проходженні автентифікації [3].

При використанні декількох (обов'язково різних) факторів та їх комбінацій автентифікація називається багатофакторною. В даній роботі для проведення багатофакторної автентифікації буде використовуватися саме соціальний фактор.

1.2. Недоліки наявних рішень для застосування багатофакторної автентифікації

За даними, опублікованими Національним Інститутом Стандартів та Технологій США (NIST) [1], використання SMS-повідомлень для проведення двофакторної автентифікації обумовлює перевіряючу сторону контролювати не лише співпадіння одноразових паролів, а і деяку суміжну інформацію. Також зазначається, що використання SMS-повідомлень є небажаним та небезпечним та в подальшому має бути усуненим від використання у якості способу доставки одноразового пароля користувачу. Це підтверджує розповсюджену серед експертів думку про те, що використання SMS-повідомлень для проведення двофакторної автентифікації не може вважатися повноцінним фактором, оскільки першочергово технологія SMS не призначалася для даної мети.

[a] karpets.as@gmail.com

Згідно з дослідженнями, використання додатку Google також не є надійним засобом для проведення автентифікації, оскільки було встановлено невідповідність згенерованих кодів стандартним тестам NIST на випадковість, а також описано можливу модель проведення атаки на дану схему [2].

Принципово нову можливість для додаткового фактору автентифікації надає нещодавно розроблена технологія блокчейн.

2. Застосування технології блокчейн для проходження автентифікації

2.1. Опис технології блокчейн

Блокчейн – це структура даних, що являє собою зв'язний список, для побудови якого замість звичайних вказівників використовуються геш-вказівники. Геш-вказівники – це структури даних, які містять в собі вказівник на місце збереження деяких даних разом з гешом цих даних. Таким чином, утворюється ланцюжок блоків даних, кожен з яких додатково містить в собі значення вказівника та значення гешу попереднього блоку. Перший блок містить в собі геш так званого генезис-блоку (genesis block), вміст якого визначається наперед. При цьому, користувач блокчейну зберігає геш-вказівник на останній блок в місці, недоступному іншим користувачам.

Завдяки своїй будові дана структура дозволяє утворити журнал із цифровим пломбуванням (tamper-evident log), тобто такий журнал, підроблення записів в якому неможливо приховати. Дана властивість досягається завдяки використанню геш-вказівників [4].

Децентралізованість та розподіленість блокчейну дозволяють використовувати його для побудови нових схем багатофакторної автентифікації.

2.2. Нова схема для проведення автентифікації

Дана схема автентифікації користувача базується на популярній схемі, що використовує комбінацію статичного та одноразового пароля (тобто, комбінацію факторів знання та володіння), при чому використовується генератор OTP з розподіленим між користувачем та сервером початковим значенням. Для підвищення стійкості даної схеми пропонується використовувати третій фактор – соціальний.

Першочергово користувач, що бажає авторизуватися на сервері, надсилає йому свої ідентифікаційні дані та статичний пароль. У разі проходження першого фактору сервер вимагатиме надсилання OTP, згенерованого з попередньо розподіленого початкового значення деяким узгодженим алгоритмом.

Наступним та фінальним етапом буде підтвердження достовірності користувача його довіреними особами, які обираються користувачем перед початком взаємодії з сервером. Вибір осіб здійснюється на основі соціальних відносин з користувачем поза межами системи. Кожен з них також є користувачем даної системи та має той самий алгоритм генерації OTP та початкове значення, що і цільовий користувач (ця умова не є обов'язковою та використовується з метою взаємодії з іншими факторами).

При підтвердженні правильності значення надісланого одноразового пароля сервер надсилає запити до довірених осіб шляхом додавання блоку з міткою згоди від сервера до блокчейну. Перевірка того, чи дійсно цільовий користувач здійснює спробу входу до системи довіреними особами відбувається поза межами системи.

Перевіривши достовірність користувача, вони генерують блоки даних, що містять їх ідентифікатори, значення OTP та мітку згоди/незгоди надання доступу. Ці блоки поетапно записуються в блокчейн.

Варто зазначити, що ланцюг блоків транзакцій на надання згоди доступний всім учасникам системи автентифікації, тому забезпечується безвідмовність роботи у випадках, коли деякі з довірених осіб відсутні чи надають хибні значення.

Остаточне рішення щодо надання доступу приймається сервером на основі переважаючої кількості міток, наданих довіреними особами.

Дана процедура забезпечує (при певних умовах) досягнення правильного висновку у випадку, коли деякі з довірених осіб відсутні або надають хибні дані про достовірність користувача.

Стійкість запропонованого принципу автентифікації в залежності від кількості обраних довірених осіб, що попередньо фіксуються користувачем, який авторизується на деякому онлайн-ресурсі є самостійною задачею досліджень. Даний аналіз проводиться з метою знаходження кількості довірених осіб, що є оптимальною з точки зору надійності системи та рівня довіри до цих осіб. Таким чином, буде знайдено компроміс між стійкістю системи та кількістю довірених осіб.

Висновки

В ході виконання даної роботи було запропоновано нову комбінацію факторів для проведення автентифікації користувачів, що дозволяє покращити захист систем від несанкціонованого доступу.

Перелік використаних джерел

1. Paul A. Grassi, James L. Fenton, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, Justin P. Richer DRAFT NIST Special Publication 80063B. Digital Identity Guidelines. — 2017.
2. М. В. Блик Аналіз практичної стійкості протоколів двофакторної автентифікації. — 2016.
3. Комаров А. Современные методы аутентификации. — 2015.
4. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. — 2015.