Висновки. Розроблений інтелектуальний алгоритм пошуку фільмів за описом дозволяє користувачам знаходити фільми, назва яких є невідома. Використання Angular на клієнтській стороні та node.js на серверній стороні дозволили реалізувати цей алгоритм. Розглянутий підхід робить пошук фільмів більш інтелектуальним та персоналізованим для кожного користувача. Алгоритм обробки природної мови (NLP) в системі пошуку фільмів за описом допомагає робити пошук більш точним та зручним. Використовуючи цей алгоритм, система враховує інтереси користувача та знаходить фільми, які найкраще відповідають їхнім вподобанням, враховуючи зміст введеного тексту опису фільмів.

Список використаних літературних джерел

[1] Документація Angular: https://angular.io/docs

[2] Документація Express.js: https://expressjs.com/

[3] Документація The Movie Database API: https://developers.themoviedb.org/3/

[4] Документація Node.js: https://nodejs.org/en/docs/

[5] Cambria E, White B (2014) Jumping NLP curves: a review of natural language processing research. IEEE Computat Intell Mag 5:48–57

Юрій Паславський, Ігор Крошний*
аспірант кафедри КН НЛТУ України, Львів, Україна.
yuriy.paslavskyy@nltu.edu.ua
*доцент кафедри КН НЛТУ України, Львів, Україна.
kroshny.igor@nltu.edu.ua

Методи використання алгоритмів неінтерактивних аргументів знання для ідентифікації користувача

Анотація - З розвитком мережевих технологій надзвичайно актуально постало завдання підвищення ефективності і захищеності схем ідентифікації з одночасним дотриманням правил безпеки, анонімності і конфіденційності. Стратегічним напрямком дій у цій сфері є запровадження алгоритмів, що мають підвищену криптографічну складність та потребують суттєвих часових витрат задля їх зламу. Для розв'язання цих завдань використовуються основні

* науковий керівник

положення методів аналізу даних, криптографії, ідентифікації; для удосконалення методів ідентифікації методи експоненціонування з використанням поліноміальної та модулярної арифметики; для реалізації інформаційної технології – методології проектування інформаційних систем та об'єктно-орієнтований підхід.

Ключові слова - ідентифікація, криптографія, анонімність, конфіденційність, докази з нульовим розголошенням, Zero-Knowledge Proof.

На даний час існує достатньо велика кількість різноманітних технологій для ідентифікації користувачів, які умовно можна розділити на дві групи.

До першої групи відносяться технології, що передбачають використання певної наперед визначеної інформації для ідентифікації користувача системою. Це, насамперед, ідентифікація за допомогою секретної інформації (пароля), технології з використанням спеціальних технологічних пристроїв (електронних карток), технології з використанням біометричних даних особи або з використанням радіочастот.

Друга група використовує технології, що передбачають імплементацію концепції «нульових знань». Згідно з цією концепцією, для кожного нового сеансу ідентифікації використовуються різні паролі, а секретна ідентифікаційна інформація зберігається лише у однієї зі сторін протоколу, найчастіше у користувача. Сутність цієї концепції полягає у можливості довести певне твердження, не розголошуючи при цьому сам доказ, навіть частково.

Технології ідентифікації, що передбачають використання паролів класифікують за ступенем частоти зміни пароля [1]:

- методи, які використовують постійні (багаторазові) паролі;
- методи, які використовують одноразові (динамічні) паролі.

Поширенішим є використання багаторазових паролів, яке спрощує процедури адміністрування, але підвищує загрозу розсекречення пароля одним із багатьох відомих на сьогодні способів. Надійнішим є використання одноразових або динамічно змінюваних паролів.

* науковий керівник

Іншим варіантом технологій регулювання доступу є використання найрізноманітніших технічних засобів, зокрема, жетонів, електронних карток тощо [2].

Також швидко розвиваються технології, що вимірюють біометричні параметри людини - фізіологічні або поведінкові (малюнком райдужної оболонки ока, відбитками пальців та долоні, формою вух, інфрачервоною картиною капілярних судин, тембром голосу, лінгвістичні характеристики та навіть ДНК). Такі технології характеризуються надзвичайно високим рівнем достовірності ідентифікації та фактично, унеможливлюють втрату пароля та/або особистого ідентифікатора. Проте такі методи потребують складного та дороговартісного спеціального обладнання [3].

Отже, найсучаснішим і найтехнологічнішим є використання ZKP - доказів з нульовим розголошенням (англ. «Zero-Knowledge Proof») - криптографічна концепція, згідно з якою, доводяча сторона має можливість довести знання певної інформації перевіряючій стороні, не розкриваючи суті самої інформації. Доказ з нульовим розголошенням не видає ніяких інших даних окрім вірності твердження і дозволяє довести це твердження, не видаючи жодної додаткової інформації про саме твердження.

Всі сучасні протоколи ідентифікації абонентів розділяють на два класи: з використанням паролів, що перевіряються системою шляхом порівняння (“слабка” ідентифікація) та на основі теоретичної концепції “нульових знань” (“сильна” ідентифікація).

Сутність цієї концепції полягає в тому, що для доведення своєї ідентичності абонент має неявним чином виявити знання певної інформації, якою система не володіє, але може перевірити її наявність у абонента. При цьому в системі не зберігається жодної секретної інформації, яка дозволяє відновити ідентифікаційні дані абонента, що пояснює походження назви концепції "нульових знань”. При кожному зверненні до системи абонентом генерується нова ідентифікуюча інформація.

* науковий керівник

Таким чином, концепція “нульових знань” найбільш повною мірою відповідає вимогам забезпечення високого рівня захищеності від спроб несанкціонованого доступу до ресурсів розподілених систем. Концепція “нульових знань” базується на використанні незворотних математичних перетворень, а саме аналітично нерозв’язуваних задачах теорії чисел, зокрема відомої задачі дискретного логарифмування.

До найбільш відомих схем ідентифікації, що відповідають концепції “нульових знань” відносяться: метод Feige Fiat Shamir Identification Scheme (FFSIS) та його модифікації Joseph Kizza та Ohta Okamoto, Guillou-Quisquater й Schnorr.

Суть методу FFSIS полягає у виборі користувачем двох простих чисел та обчисленні їх модуля. Для генерації відкритого та закритого ключів користувач вибирає інше число, що є квадратичним лишком цього модуля.

Однак, найбільш значимими для практики недоліками схеми ідентифікації FFSIS є необхідність в декількох циклах акредитації, що, в свою чергу, потребує значної кількості сеансів передачі даних, а відповідно і більше часу, який суттєво залежить від поточного трафіку в комп’ютерній мережі і на порядки перевищує час виконання системою обчислень, пов’язаних з ідентифікацією користувача. Велика кількість коротких сеансів передачі даних при ідентифікації кожного користувача значно впливає на пропускну здатність мережевого інтерфейсу системи. Крім того, наявність прогнозованих декількох сеансів передачі даних з конкретним користувачем відкриває потенціальні можливості для зловмисників ефективно завадити успішному проведенню циклу ідентифікації.

Для покращення методу FFSIS розроблено декілька модифікацій: модифікація Joseph Kizza, модифікація Ohta Okamoto та методи Guillou-Quisquater і Метод Schnorr [1-2].

Модифікація Joseph Kizza покликана вирішити проблему «пінг-понгу» (ping-pong problem). Проблема "пінг-понгу" в рішеннях концепції нульових знань обумовлена багаторазовими, іноді неконтрольованими обмінами «запит-

* науковий керівник

відповідь» між Системою та Користувачем і призводить до високої ресурсомісткості процедури.

Модифікація Ohta Okamoto вирішує проблему компромісу між розміром необхідної пам'яті та розміром інформації, що передається при взаємодії Користувача з Системою. Проблема вирішується введенням третього параметр в рівняння. Дана модифікація є повільнішою за класичний метод FFSIS, але потребує значно менших ресурсів пам'яті і може ефективно застосовуватись в системах, що працюють з малопотужними терміналами, пристроями або смарт-картками.

Крім методу FFSIS та його модифікацій, широкого розповсюдження в системах колективного доступу набув метод Guillou-Quisquater, який також реалізує теоретичну концепцію строгої ідентифікації "нульових знань" [2]. Даний протокол має три властивості – повнота, коректність та нульове розголошення [3]. Протоколом передбачено тільки один цикл обміну повідомленнями між системою та користувачем за один цикл акредитації, проте виконує на три порядки більше обчислень, аніж при використані FFSIS. Також протокол Guillou-Quisquater в порівнянні з FFSIS, має меншу кількість повідомлень обміну задля ідентифікації.

Недоліком зазначеного методу є потреба у декількох сеансах обміну даними з одночасною потребою у виконанні операції модулярного експоненціювання користувачем безпосередньо в процесі ідентифікації, що призводить до значного збільшення часу ідентифікації користувача. Безпека протоколу базується на складності обчислення квадратного кореня по модулю для достатньо великого числа із заданим модулем.

Метод Schnorr також передбачає вибір користувачем двох простих чисел і особливістю цього методу ідентифікації є реалізація концепції "нульових знань" з використання групи чисел менших відносно невеликої розрядності, що дозволяє суттєво зменшити обчислювальну складність операцій. Суттєвою вадою методу є те, що цикл ідентифікації віддаленого користувача потребує

* науковий керівник

трьох сеансів обміну даними між користувачем та системою, що помітним чином уповільнює процес ідентифікації.

Ще одним методом є використанням незворотних перетворень на полях Галуа, утворюючи поліном який є поліноміальним добутком двох простих поліномів з різними степенями, що дозволяє значно прискорити час виконання програм та спростити апаратну реалізацію.

Висновок. З вищенаведеного аналізу існуючих методів, технологій та технологічних рішень найкращим методом є реалізація концепції «нульових знань» з використанням методу експоненціювання застосовуючи апарат поліноміальної арифметики.

Список використаних літературних джерел

[1] Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C./ Schneier B. / Ed. John Wiley. NY, - 1996, - P.758

[2] Peng K. Attack against a batch zero-knowledge proof system./Peng K. // IET Information Security — IET, 2012. — Vol. 6, Iss. 1. — PP. 1–5. — ISSN 1751-8709 — doi:10.1049/IET-IFS.2011.0290

[3] Карпанасюк В.В., Пасічник О.А. Інформаційна технологія ідентифікації користувачів. Тези доп. XI Міжнародної науково-практичної конференції «EURASIAN SCIENTIFIC CONGRESS», 1-3 листопада 2020 р. - Барселона, Іспанія, 2020. – С. 216 – 222.

Богдан Воробель, Ірина Борецька*, Богдан Бекас*, Мар'ян Опришко*
магістрант, НЛТУ України, Львів, Україна, Vorobel.b@nltu.lviv.ua.
*завідувач кафедри КН, НЛТУ України, Львів, Україна, Iryna.Boretska@Gmail.Com.
*старший викладач кафедри ІСКМ, НЛТУ України, Львів, Україна, Bohdan.Bekas@nltu.edu.ua.
*асистент кафедри ІПЗ, НЛТУ України, Львів, Україна, M.Opryshko@nltu.edu.ua

Розроблення застосунку "Інтелектуальна система створення шаблонів документів підприємця"

* науковий керівник