DOI 10.31891/2307-5732-2024-345-6-35
УДК 004.023

ТІТОВА ВІРА
Хмельницький національний університет
https://orcid.org/0000-0001-8668-4834
e-mail: titovav@khmnu.edu.ua
КЛЬОЦ ЮРІЙ
Хмельницький національний університет
https://orcid.org/0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
ПИРЧ ОЛЕНА
Хмельницький національний університет
e-mail: oleksukolena@gmail.com
ШЕМЧУК УЛЯНА
Хмельницький національний університет
e-mail: shemshyk123@gmail.com
БОЖОК ДМИТРО
Хмельницький національний університет
e-mail: dimasbmw369@gmail.com

АНАЛІЗ СУЧАСНИХ МЕТОДІВ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

У даній статті проведено аналіз існуючих методів автентифікації. До таких можна віднести: парольну аутентифікацію, аутентифікацію через сторонній ресурс, аутентифікацію за допомогою графічних паролів, аутентифікацію за допомогою одноразових та динамічних паролів, механізми аутентифікації з використанням сторонніх програмних та апаратних токенів, методи багатофакторної аутентифікації та криптографічні. Порівняння аналізованих методів проведено за трьома основними групами характеристик: зручністю використання, складністю реалізації та безпеки рішення.

У результаті проведеного порівняльного аналізу виявлено найперспективніший підхід – підхід із використанням криптографічних засобів, що забезпечує високий рівень захисту інформації.

Ключові слова: аутентифікація користувачів, методи аутентифікації, криптографічна стійкість, електронний цифровий підпис.

TITOVA VIRA, KLOTS YURII, PYRCH OLENA, SHEMCHUK ULIANA, BOZHOK DMYTRO
Khmelnitskyi National University

ANALYSIS OF MODERN USER AUTHENTICATION METHODS

There are a number of problems in modern asymmetric cryptosystems. They are mostly related to issues of cryptographic stability and acceptable key lengths. The capabilities of computing resources increase every year, which allows legitimate users to receive, process and transmit information faster, but cryptanalysts also remain in the plus - the probability of breaking existing schemes increases, and the time spent by this process decreases. Because of this, there is a constant need to increase the size of the keys, which negatively affects performance.

Due to the above, it can be seen that the so-called combined systems will be an interesting and more than relevant development. Such systems provide double protection: in addition to the standard encryption key, which is widely used in modern cryptosystems, a double protection scheme is provided.

This article analyzes existing authentication methods. These include: password authentication, authentication through a third-party resource, authentication using graphic passwords, authentication using one-time and dynamic passwords, authentication mechanisms using third-party software and hardware tokens, multi-factor authentication, and cryptographic methods. The comparison of the analyzed methods is based on three main groups of characteristics: ease of use, complexity of implementation and security of solutions.

As a result of the comparative analysis, the most promising approach was determined - an approach using cryptographic means, which provides a high level of information protection.

Keywords: user authentication, authentication methods, cryptographic stability, electronic digital signature.

Постановка проблеми

У сучасному інформаційно-розвиненому суспільстві з кожним роком все більша увага як з боку держави, так і з боку приватних компаній починає приділятися цілісності інформації, що передається, аутентифікації користувачів та іншим аспектам інформаційної безпеки. Забезпечити автентичність, доступність і цілісність інформації, що передається, дозволяє електронний цифровий підпис (ЕЦП). В даний час існує велика кількість алгоритмів та протоколів ЕЦП. Найважливішим аспектом застосування підпису є його криптостійкість, яка ґрунтується на складності обчислення будь-якої односторонньої математичної функції. Поява ефективних методів вирішення того чи іншого завдання спричинить зниження стійкості всього криптоалгоритму.

У 2016 році Національний інститут стандартів та технологій США (NIST) оголосив конкурс на створення нових стандартів шифрування, ЕЦП та обміну ключами. Вирішенням цього питання можуть стати, так звані, комбіновані схеми. Такі схеми припускають подвійний захист: створення алгоритмів і протоколів, заснованих одночасно на кількох складно обчислюваних завданнях.

Формулювання цілей статті

У сучасних асиметричних криптосистемах існує низка проблем. Здебільшого вони пов'язані з питаннями криптографічної стійкості та прийнятною довжиною ключів. Можливості обчислювальних ресурсів з кожним роком збільшуються, що дозволяє легітимним користувачам отримувати, обробляти та передавати інформацію швидше, але й криптоаналітики залишаються у плюсі – ймовірність злому існуючих схем збільшується, а час, витрачений на цей процес, зменшується. Через це виникає постійна потреба у збільшенні розмірності ключів, що негативно позначається на продуктивності.

В силу всього вище викладеного, можна бачити, що цікавою і більш ніж актуальною розробкою будуть так звані комбіновані системи. Такі системи передбачають подвійний захист: крім стандартного ключа шифрування, який повсюдно застосовується в сучасних криптосистемах, передбачається подвійна схема захисту.

Огляд існуючих рішень

Існує велика кількість методів автентифікації. Для порівняльного аналізу виділяється кілька основних груп методів. Варто відзначити, що в кожній із груп можуть бути різні реалізації, що відрізняються одна від одної конкретними характеристиками, а також сильними та слабкими сторонами. У цьому самі показники і тенденції груп, зазвичай, залишаються незмінними.

Найбільш популярним і простим методом, безперечно, можна назвати парольну автентифікацію. Вона використовується в соціальних мережах, платіжних системах, на форумах і на веб-ресурсах, що містять персональні дані. Під паролем мається на увазі спеціальна кодова фраза або набір фраз кожного ресурсу.

Розвитком даного методу є графічні паролі, що базуються на введенні певного нетекстового змісту. Переваги даних методів полягають у спрощенні запам'ятовування таких кодових елементів.

Наступною групою є методи з використанням одноразових та динамічних паролів, наприклад,GrIDsure [1]. Вони вимагають від користувача додаткових дій, але дозволяють посилити захист від атак, що базуються на повторенні паролів.

Також часто використовуваним способом є методи, засновані на аутентифікації за допомогою стороннього ресурсу або децентралізованої аутентифікації, наприклад,OpenID [2] таOAuth [3].

Наступною категорією методів є токени, сюди належать механізми аутентифікації з використанням сторонніх програмних та апаратних токенів.

Методи багатофакторної аутентифікації складають окрему категорію, сюди відносяться, наприклад, механізми з підтвердженням коду через SMS-повідомлення.

Криптографічні методи аутентифікації виділені в окрему категорію, що включає способи від використання сертифікатів до підходів стеганографічних [4].

До останньої категорії віднесено методи біометричної аутентифікації [5] на веб-ресурсі, наприклад, з використанням голосового підтвердження або на основі характеристик введення користувача.

Порівняння проводиться за трьома основними групами характеристик: зручністю використання, складністю реалізації та безпеки рішення.

У таблицях 1-3 цифрою 1 позначено найгірший показник, 2 - середній, 3 – найкращий.

До першої групи належать складність запам'ятовування кодового значення, необхідність наявності допоміжного пристрою, виконання додаткових дій, складність освоєння методу, середній час аутентифікації, частота помилок та складність відновлення аутентифікатора у разі втрати (Таблиця 1).

До другої групи належать характеристики доступності методу, вартості рішення, вимоги до серверної та клієнтської архітектури, а також пропрієтарність методів (Таблиця 2).

До третьої групи відносять стійкість методів до атак перебором, цільового та нецільового спостереження, атак за допомогою непрямого злому, фішингових атак та фізичної крадіжки (Таблиця 3).

Таблиця 1

Порівняння методів автентифікації за зручністю користування

Зручність використання							
	Запамя-товування	**Доп. пристрій**	**Викон. дій**	**Легкість**	**Час**	**Помилки**	**Відновлення**
Пароль	1	3	2	3	3	2	3
Сторонній ресурс	2	3	3	3	3	3	2
Графічні	1	1	2	3	3	2	3
Динамічні	1	3	2	2	3	2	2
Токени	3	1	1	1	2	3	1
Багатофакторна	1	1	1	3	2	2	1
Криптографія	3	1	1	1	1	2	1
Біометрія	3	3	2	3	2	2	1

Таблиця 2

Порівняння методів аутентифікації за простотою реалізації

	Реалізація				
	Доступність	**Вартість**	**Серверна середовище**	**Клієнтське середовище**	**Пропрієтарність**
Пароль	3	3	3	3	3
Сторонній ресурс	3	3	1	3	3
Графічні	1	3	1	3	3
Динамічні	2	3	2	2	3
Токени	1	1	1	2	1
Багатофакторна	2	2	2	2	2
Криптографія	1	1	1	2	1
Біометрія	1	1	1	1	1

Таблиця 3

Порівняння методів автентифікації з безпеки даних, що передаються

	Безпека				
	Перебір	**Спостереження**	**Непрямий злом**	**Фішинг**	**Крадіжка**
Пароль	1	1	1	1	3
Сторонній ресурс	2	2	3	3	3
Графічні	1	1	2	2	3
Динамічні	2	3	2	2	3
Токени	3	3	3	3	2
Багатофакторна	1	1	3	3	2
Криптографія	3	3	3	3	3
Біометрія	3	3	1	1	3

Зі сказаного вище можна бачити, що автентифікація з використанням простих паролів найбільш легка в реалізації, але не дуже безпечна, і вимагає постійного запам'ятовування паролів.

Методи використання аутентифікації через сторонні ресурси дуже зручні для користувачів, але вимагають певних налаштувань сервера, а їх безпека заснована на захищеності провайдера даної послуги.

Графічні та динамічні паролі дозволяють трохи збільшити захищеність від різних видів загроз, однак це ускладнює використання та збільшує вимоги до клієнтських та серверних реалізацій.

Методи захисту з використанням токенів є порівняно безпечними, але потребують спеціалізованих налаштувань, а також найчастіше є пропрієтарними та платними.

Двофакторна аутентифікація з використанням мобільних пристроїв дещо знижує зручність використання, але різко підвищує захищеність від деяких видів атак, однак, це призводить до необхідності ускладнення серверної архітектури та вимагає від користувача додаткових дій.

Криптографія та біометрія є найбільш захищеними підходами, але зручність використання та складність реалізації гірша, ніж у інших методів.

З порівняльного аналізу можна побачити, що немає ідеального методу аутентифікації. Кожне поліпшення характеристик безпеки методу тягне за собою погіршення характеристик зручності використання, або призводить до ускладнення клієнтської та серверної архітектур. У результаті, для кожного ресурсу потрібно використовувати метод найбільш підходящий до конкретної ситуації та вимог власників ресурсу, враховуючи ризики, загрози та цінність інформації, що захищається.

Лідером зручності використання є методи аутентифікації через третю сторону, куди відносяться також і децентралізовані підходи. Дані методи, наприклад, OAuth та OpenID широко використовуються в Інтернет і дозволяють легко проводити аутентифікацію на будь-яких ресурсах з використанням всього одного пароля, однак вони природно мають не такий високий рівень безпеки, хоча і більш надійні, ніж традиційні підходи.

Найбільш простим для реалізації є паролі, однак така властивість обумовлена зменшенням захищеності та зручності використання кінцевими користувачами.

Однак якщо говорити про захист критично важливих веб-інфраструктур, то з точки зору безпеки обґрунтованим є використання криптографічних або біометричних методів автентифікації. Але нині біометричні методи є недостатньо розвиненими на веб-ресурсах.

Подальший розвиток кожного методу має природні обмеження, і тенденції їхнього подальшого вдосконалення лежать у сфері комбінованих систем. Цікавим для розгляду є підходи, що використовують криптографічні прийоми для вирішення задач аутентифікації, оскільки можуть розширювати можливості інших методів.

Висновки

В дані статті проведено аналіз існуючих методів аутентифікації у мережі Інтернет. Виявлено найбільш перспективний підхід – підхід із використанням криптографії, що забезпечує високий рівень захисту для критично важливої інформації. Показано, що здійснювати процедуру автентифікації на веб можна за допомогою електронного підпису.

Проаналізовано існуючі наразі схеми електронної підпис. Синтезовано основні складні завдання з теорії чисел, що лежать у їх основі. Наведено оцінку їх криптостійкості.

Виявлено основні проблеми сучасних криптосистем. Обґрунтовано високу затребуваність та актуальність розробки нових комбінованих схем ЕЦП.

Література

1. Grid Authentication [Електронний ресурс] – Режим доступу: https://safenet.gemalto.com/multi factor-authentication/authenticators/grid-authentication.

2. Open ID foundation [Електронний ресурс] – Режим доступе: http://openid.net.

3. OAuth 2.0 [Електронний ресурс] – Режим доступе: https://oauth.net/2.

4. Mozhaiev, O., Gnusov, Y., Manzhai, O., Strukov, V., Nosov, V., Radchenko, V. i Yenhalychev, S. (2023) «Стеганографічний метод захисту акустичної інформації у системах критичного застосування», СУЧАСНИЙ СТАН НАУКОВИХ ДОСЛІДЖЕНЬ ТА ТЕХНОЛОГІЙ В ПРОМИСЛОВОСТІ, (3 (25), с. 52–63. doi: 10.30837/ITSSI.2023.25.052.

5. Ляшенко, Г.Є & Астраханцев, А.А. (2017). Дослідження ефективності методів біометричної автентифікації. Системи обробки інформації. 2(148). 111-114. 10.30748/soi.2017.148.20.

References

1. Grid Authentication [Elektronnyi resurs] – Rezhym dostupu: https://safenet.gemalto.com/multi factor-authentication/authenticators/grid-authentication.

2. Open ID foundation [Elektronnyi resurs] – Rezhym dostupe: http://openid.net.

3. OAuth 2.0 [Elektronnyi resurs] – Rezhym dostupe: https://oauth.net/2.

4. Mozhaiev, O., Gnusov, Y., Manzhai, O., Strukov, V., Nosov, V., Radchenko, V. i Yenhalychev, S. (2023) «Stehanohrafichnyi metod zakhystu akustychnoi informatsii u systemakh krytychnoho zastosuvannia», SUChASNYI STAN NAUKOVYKh DOSLIDZhEN TA TEKhNOLOHII V PROMYSLOVOSTI, (3 (25), s. 52–63. doi: 10.30837/ITSSI.2023.25.052.

5. Liashenko, H.Ie & Astrakhantsev, A.A. (2017). Doslidzhennia efektyvnosti metodiv biometrychnoi avtentyfikatsii. Systemy obrobky informatsii. 2(148). 111-114. 10.30748/soi.2017.148.20.