UDC 655+004.056 https://doi.org/10.15407/pp2026.03.029

R.A. Diakiv, Y.M. Kavyn

ANALYSIS OF PASSWORD AUTHENTICATION STRENGTH

The article develops an approach to assessing the strength of password authentication based on numerical, probabilistic, and entropy metrics. For this purpose, mathematical expressions were formulated to determine the time required to crack a password using brute-force methods, as well as the probability of successfully guessing it within its validity period. The proposed formulas made it possible to identify the key parameters affecting password security, including length, alphabet size, character complexity, and password lifetime.
Particular attention is paid to the analysis of password entropy according to Shannon and heuristic entropy recommended by NIST. Based on these approaches, criteria were established for determining whether a password can be considered resistant to attacks. To confirm the research results, examples of entropy calculations for different password lengths and alphabets were provided, along with statistical data on password usage in Google services. This made it possible to reveal that a significant number of users continue to employ overly simple combinations that are highly vulnerable to attacks.
In addition, the article presents a comparative analysis of traditional approaches and modern methods for improving security. In particular, the integration of classical password-based methods with new technologies, such as graphical passwords and steganographic mechanisms based on digital watermarks, is proposed. This approach makes it possible to enhance the robustness of authentication systems and provide additional protection against unauthorized access to information resources.
Keywords: authentication, password methods, information networks, unauthorized access, information security, brute-force method, entropy, Shannon, integrated systems.

Р.А. Дяків, Я.М. Кавин

АНАЛІЗ СТІЙКОСТІ ПАРОЛЬНОЇ АУТЕНТИФІКАЦІЇ

У статті було розроблено підхід до оцінки стійкості парольної аутентифікації на основі чисельних, імовірнісних та ентропійних метрик. Для цього були сформульовані математичні вирази, що дозволяють визначати час, необхідний для зламу пароля методом повного перебору, а також імовірність його підбору протягом терміну дії. Запропоновані формули дали можливість окреслити ключові параметри, які впливають на рівень захисту паролів: довжину, розмір алфавіту, складність символів та час їх актуальності.
Окрему увагу приділено аналізу ентропії парольних виразів за Шенноном та евристичної ентропії, рекомендованої NIST. На основі цих підходів були визначені критерії, за якими можна вважати пароль стійким до зламу. Для підтвердження результатів дослідження були наведені приклади обчислення ентропії при різній довжині та алфавіті, а також статистичні дані щодо використання паролів у сервісах Google. Це дозволило виявити, що значна кількість користувачів продовжує застосовувати надто прості комбінації, які легко піддаються атакам.
Крім того, у статті було здійснено порівняльний аналіз традиційних підходів та сучасних методів підвищення безпеки. Зокрема, запропоновано інтеграцію класичних парольних методів із новими технологіями, такими як графічні паролі та стеганографічні механізми на основі цифрових водяних знаків. Це дає змогу підвищити рівень стійкості системи аутентифікації та забезпечити додатковий захист від несанкціонованого доступу до інформаційних ресурсів.
Ключові слова: аутентифікація, парольні методи, інформаційні мережі, несанкціонований доступ, захист інформації, метод «грубої сили», ентропія, Шеннон, інтегровані системи.

Problem statement

In modern information and communication systems, user authentication plays a key role, as the level of data security and protection against unauthorized access directly depends on its reliability. In the previous part of the thesis, various authentication methods were examined in detail, particularly password-based systems which, despite their relatively low resilience, remain the most widespread means of identity verification. This is primarily due to their simplicity and convenience for users, who often neglect recommendations for creating strong passwords [1].

© Р.А. Дяків, Я.М. Кавин, 2026

CC BY 4.0

At the same time, the conducted analysis demonstrated that password authentication is highly vulnerable to attacks, since many users choose overly simple and predictable combinations. The use of brute-force and dictionary attacks, combined with increasing computational power, enables the rapid cracking of low-complexity passwords. Even developed mathematical security metrics — numerical, probabilistic, and entropy-based — indicate that the actual level of password protection is significantly lower than desired. This is further confirmed by statistical data from leaked password databases of well-known services.

Despite these obvious shortcomings, password-based methods remain relevant and require further improvement [2]. One promising direction for increasing their effectiveness is the development of integrated systems that combine classical password authentication with additional protection mechanisms. In particular, approaches based on entropy analysis, the creation of more complex password expressions, and the use of additional security factors are considered перспективними.

At the same time, the implementation of innovative solutions, including graphical passwords and steganographic methods, is becoming an increasingly relevant research direction. The use of digital watermarks in identification systems opens new possibilities for generating one-time passwords, significantly complicating unauthorized access attempts. These approaches will be discussed in the next section of the work.

Analysis of recent publications and research

Recent publications and studies in the field of authentication approaches emphasize the importance of improving password protection methods. Among the key issues highlighted is the lack of a unified approach to evaluating the resilience of password systems. This creates serious vulnerabilities for information resources, as users often fail to follow basic password creation recommendations. In particular, statistics indicate numerous cases of password leaks from well-known services, which stimulates further research in this area [3]. Researchers analyze password-cracking expressions, focusing on the time required for brute-force attacks and the importance of constructing passwords with sufficient length and character diversity.

Purpose of the article

The purpose of this article is to investigate the strength of password authentication in applied systems. The author aims to identify the main parameters that influence password reliability, including password length, complexity, and alphabet diversity. Particular emphasis is placed on analyzing password phrases through the lens of entropy, which allows the resistance of passwords to attacks to be evaluated. Since there is extensive statistical data regarding password usage, the article also highlights the necessity of integrating new methods for protecting information resources while taking modern threats into account. As a result, the author hopes to contribute significantly to the development of more secure and user-friendly authentication systems.

Presentation of the Main Material

One of the directions in the development of authentication approaches is the improvement of password-based methods. At the same time, two main requirements remain essential: ensuring a high level of security for information networks and maintaining simplicity and ease of use.

This article examines the issue of password authentication strength in applied systems. This issue has not yet been fully investigated, since developers do not have a unified approach to evaluating the resilience of password systems [4]. Users, due to the simplicity of use, prefer password-based protection; however, in many cases, they fail to comply with even basic requirements for password creation. As a result, information resources remain vulnerable, and there is a high probability of unauthorized access [5]. In recent years, password database leaks from

many well-known services, such as Google, Mail, and Dropbox, have occurred, giving new impetus to research on the resilience of password protection systems.

Let us analyze the expressions used for password cracking. An expression was studied for calculating the time *T* required to guarantee the cracking of a password of a given length using the brute-force method. Based on this expression, a probabilistic expression for password recognition was developed.

$$P = \frac{V \cdot T}{A^n}, \quad (1)$$

where V - password cracking speed by an attacker;

T - the period during which the password is valid;

n - number of characters in the password;

A^n - the maximum possible number of password combinations for a given length and alphabet size (calculated based on the exponential law of information quantity).

Expression (1) indicates that the reliability of a password depends on the password guessing speed, the set of all possible password combinations, the number of characters in the password, and the alphabet used in its formation.

The expression presented in (2) makes it possible to define a list of password parameters and requirements under which a password will possess an acceptable level of resistance to cracking. The first parameter is the number of characters in the password, or the password length. From the standpoint of both security and ease of memorization, a length of 8 characters is generally considered acceptable. According to the exponential law, the larger the alphabet (letters, numbers, symbols, uppercase and lowercase characters), the greater the number of possible messages that can be generated. In this case, increasing the number of possible combinations increases the time required for brute-force attempts and, consequently, improves password resistance to cracking. In addition, to increase security, a password should not contain any meaningful word or its part, people's names or surnames, or any common titles and designations [6].

At the same time, there is no unified methodology in the scientific literature for analyzing password strength. Among the most commonly used measures are numerical, probabilistic, heuristic, and other metrics.

Determining the time required for exhaustive password search belongs to numerical metrics. The disadvantage of this approach is that it does not take into account intelligent methods of password phrase guessing. Expression (1) represents a probabilistic metric of password protection. The drawback of this approach is that researchers do not always have access to the statistical data necessary for calculations using expression (1).

Let us analyze password phrases using Shannon entropy and heuristic entropy recommended by the U.S. National Institute of Standards and Technology. The difference between these numerical analysis approaches lies in their different views on the nature of password creation. One approach assumes that passwords are generated randomly, whereas heuristic entropy assumes that the password phrase is created by a human [7].

The expression for calculating the entropy of password phrases according to Shannon is as follows:

$$H = \log_2 |A|^n = n \cdot \log_2 |A| = n \cdot \frac{\ln A}{\ln 2}, \quad (2)$$

where $|A|^n$ - maximum possible number of passphrase options;

n - number of characters in the passphrase.

Thus, metric (2) demonstrates that the greater the number of possible password phrase combinations — namely, the larger the alphabet size and the greater the number of characters in the password — the more resistant the password is to cracking.

An example of Shannon entropy calculation for different alphabet sizes and password lengths is presented in Table 1:

Table 1.

Calculation of Shannon entropy for passphrases.

Alphabet/length	5	6	7	8
Latin alphabet	23.5	28.2	32.9	37.6
Numbers	16.6	19.9	23.2	26.5
Latin alphabet + uppercase + numbers	29.7	35.7	41.6	47.6
Latin alphabet + Cyrillic + uppercase + numbers	35	41.9	48.9	55.9

Heuristic entropy is calculated using the following expression:

$$S(A,n) = 4 + \sum_{i=2}^{8} 2 + \sum_{i=9}^{20} 1{,}5 + \sum_{i=21}^{n} 1 + 6 \cdot \chi_A , \quad (3)$$

where $i \le n$, n - password length, χ_A - a characteristic feature of the presence of non-alphabetic or uppercase characters in the password.

Expression (3) is described as follows. The first password character is assigned a value of 4 bits, each subsequent character from the second to the eighth contributes 2 bits, characters from the ninth to the twentieth contribute 1.5 bits each, and every following character contributes 1 bit [8]. If the password contains non-alphabetic characters or uppercase letters, an additional 6 bits are added to the resulting value.

According to the presented metrics (2) – (3), a password phrase is considered strong if its entropy is 56 bits or more (according to Shannon) or 24 bits or more (according to the recommendations of the National Institute of Standards and Technology).

These metrics have a number of limitations. For example, if a password is included in password-cracking databases, its entropy becomes equal to zero.

Let us consider some statistical characteristics of Google passwords (Table 2).

Table 2.

Statistics on the number of passwords of a given length in Google

Password lenth	*Number of passwords*
6	924154
7	663510
8	1422999
9	683315

10	682811
11	152256
12	93202
13	42387
14	24853
15	14851
16	7291
17	2549
18	1781
19	1082
20	1166

A large number of passwords are repeated. This mostly applies to very simple passwords. Table 3 shows Google statistics.

Table 3.

Statistics of repeated passwords in Google

Password	*Number of repetitions*
123456	47918
password	11554
123456789	11160
12345	8096
querty	5918
12345678	5250
111111	3521
abc123	3011
123123	2972
1234567	2911

There are also known statistics regarding the use of passwords with different alphabets.

Alphabet used	*Number of passwords*
Numbers only	774669
Symbols only	1968873
Matches login	45010
Shannon entropy-resistant	290530
NIST compliant	157475

Based on the analysis of the statistical information presented in Tables 1–3, a slight improvement in password protection against cracking can be observed. This improvement is explained by the strengthening of requirements imposed by a number of Internet resources regarding the minimum parameters of password phrases, namely password length and alphabet size. At the same time, as shown by the data in Table 3, there remains a large number of users who create overly simple passwords that can be guessed quite easily [9].

In general, the conducted analysis of password-based methods demonstrates that this type of authentication is rather vulnerable, since fewer than 10% of passwords can be considered resistant to attacks. At the same time, as noted above, password authentication remains widespread among users due to its convenience and ease of use. This necessitates the development of integrated information resource protection systems based on password authentication with enhanced resistance to cracking.

Methods for constructing graphical password systems using steganographic techniques are known, particularly those based on digital watermarks, which are applied in identification/authentication systems as one-time passwords for user authorization and access to information resources [10].

Conclusions

The article presents a comprehensive analysis of password authentication methods and evaluates their resistance to cracking. It was established that, despite their simplicity and ease of use, most passwords chosen by users do not meet security requirements, which is confirmed by statistical data from well-known services. Mathematical modeling of password brute-force attacks, along with entropy analysis according to Shannon and the recommendations of the National Institute of Standards and Technology, demonstrated that fewer than 10% of passwords can be considered truly secure.

The developed numerical, probabilistic, and entropy-based metrics made it possible to determine the key parameters influencing password strength, namely password length, alphabet size, and character complexity. It was shown that increasing these parameters significantly complicates password guessing using brute-force methods. At the same time, limitations of traditional approaches were identified, particularly the failure to account for dictionary attacks and the human factor in password creation.

The study emphasizes the feasibility of using integrated protection systems that combine classical password authentication with modern technologies. The use of graphical passwords and steganographic methods, particularly digital watermarks that can function as one-time passwords, is considered a promising direction. This opens up opportunities for improving the security level of information resources and minimizing the risks of unauthorized access.

References

1. Bonneau, J. (2012). *The science of guessing: Analyzing an anonymized corpus of 70 million passwords*. In *2012 IEEE Symposium on Security and Privacy* (pp. 538–552). IEEE. https://doi.org/10.1109/SP.2012.49
2. Florêncio, D., & Herley, C. (2007). *A large-scale study of web password habits*. In *Proceedings of the 16th International Conference on World Wide Web* (pp. 657–666). ACM. https://doi.org/10.1145/1242572.1242661
3. Shay, R., Komanduri, S., Durity, A. L., Huh, P. S., Mazurek, M. L., Segreti, S. M., Ur, B., Bauer, L., Christin, N., & Cranor, L. F. (2014). *Can long passwords be secure and usable?* In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2927–2936). ACM. https://doi.org/10.1145/2556288.2557377
4. Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). *Graphical passwords: Learning from the first twelve years*. *ACM Computing Surveys, 44*(4), 1–41. https://doi.org/10.1145/2333112.2333114
5. Johnson, N. F., Duric, Z., & Jajodia, S. (2001). *Information Hiding: Steganography and Watermarking—Attacks and Countermeasures*. Boston, MA: Kluwer Academic Publishers. https://doi.org/10.1007/978-1-4615-0359-0
6. Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2007). *Digital Watermarking and Steganography* (2nd ed.). Burlington, MA: Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-372585-1.X5001-3
7. Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). *Information hiding—A survey*. *Proceedings of the IEEE, 87*(7), 1062–1078. https://doi.org/10.1109/5.771065
8. Harris, S., & Maymi, F. J. (2021). *CISSP All-in-One Exam Guide* (9th ed.). New York, NY: McGraw-Hill Education.
9. Stolitnyi, O. V. (2019). *Information protection in computer systems and networks*. Kyiv: Igor Sikorsky Kyiv Polytechnic Institute.
10. Markov, A. S., Tsirlov, V. L., & Barabanov, A. V. (2012). *Methods for assessing the inadequacy of information protection measures*. Moscow: Radio and Communications.

Дата першого надходження до видання: 23.05.2026
Внутрішня рецензія отримана: 18.06.2026
Зовнішня рецензія отримана: 20.06.2026
Дата прийняття до друку: 10.08.2026
Дата публікації: 29.08.2026

About authors:

[1]Дяків Роман Андрійович, аспірант
*[1]*Diakiv Roman, PhD student
https://orcid.org/0009-0000-8113-7110.

*[2]*Кавин Ярослав Михайлович,
доцент, кандидат технічних наук
*[2]*Kavyn Yaroslav,
associate professor, candidate of technical sciences
https://orcid.org/0009-0001-9583-8679.

Place of work:

*[1]*Національний університет «Львівська політехніка»
*[1]*Lviv Politechnic National University
Phone: +380937510325
E-mail: roman.a.diakiv@lpnu.ua

*[2]*Національний університет «Львівська політехніка»
*[2]*Lviv Politechnic National University
Phone: +380989533061
E-mail: yaroslav.m.kavyn@lpnu.ua