CIENTIFICA
TechNoLogica
ISSN:3119-7906, Vol.1Núm.2(2026): Abril-Junio
https://doi.org/10.17268/tech1.2.2026.05

Aplicación del Algoritmo de Fuerza Bruta en la Evaluación de la Seguridad de Contraseñas Electrónicas

Application of the Brute Force Algorithm in the Evaluation of Electronic Password Security

Álvarez Marchena Manuel Jose[1], Gamarra Ventura Yesenia[1], Palomino Capristan Josue Alexander[1], Quiroz Torres Cielo Briguitte[1], Reaño Hernández Marco Antonio [1]

[1] Escuela de Ingeniería Informática, Universidad Nacional de Trujillo, La Libertad, Perú

*Autor correspondiente: malvarezm@unitru.edu.pe (Manuel. A)

RESUMEN

La creciente dependencia de los sistemas electrónicos ha incrementado la importancia de la seguridad informática y la protección de las credenciales de acceso. En este contexto, el presente trabajo tuvo como objetivo analizar la aplicación del método de fuerza bruta en la protección de contraseñas electrónicas, considerando su funcionamiento, los factores que influyen en su efectividad y las principales estrategias de seguridad utilizadas para prevenir accesos no autorizados. La investigación se desarrolló mediante un estudio documental y descriptivo basado en la revisión de literatura especializada, estándares internacionales y documentos técnicos relacionados con la ciberseguridad y los mecanismos de autenticación. Los resultados permitieron identificar que la longitud y complejidad de las contraseñas influyen directamente en su resistencia frente a ataques de fuerza bruta, así como determinar que mecanismos como las funciones hash, el salting, la autenticación multifactor y el empleo de algoritmos especializados, tales como PBKDF2, bcrypt, scrypt y Argon2, contribuyen significativamente a fortalecer la seguridad de las credenciales.

Palabras clave: Fuerza bruta, seguridad informática, contraseñas electrónicas, autenticación, ciberseguridad.

ABSTRACT

The increasing dependence on electronic systems has heightened the importance of information security and the protection of access credentials. In this context, the objective of this study was to analyze the application of the brute-force method in the protection of electronic passwords, considering its operation, the factors affecting its effectiveness, and the main security strategies used to prevent unauthorized access. The research was conducted through a documentary and descriptive study based on the review of specialized literature, international standards, and technical documents related to cybersecurity and authentication mechanisms. The results showed that password length and complexity directly influence their resistance to brute-force attacks and revealed that mechanisms such as hash functions, salting, multi-factor authentication, and the use of specialized algorithms such as PBKDF2, bcrypt, scrypt, and Argon2 significantly strengthen credential security.

Keywords: *Brute force, information security, electronic passwords, authentication, cybersecurity.*

I. INTRODUCCIÓN

El avance de las tecnologías de la información y la transformación digital han incrementado la dependencia de los sistemas electrónicos para el almacenamiento y procesamiento de información sensible. En este contexto, la seguridad informática constituye un elemento fundamental para garantizar la confidencialidad, integridad y disponibilidad de los datos. Según Stallings [1], los mecanismos de autenticación basados en contraseñas continúan siendo uno de los métodos más utilizados para controlar el acceso a sistemas y servicios digitales, debido a su facilidad de implementación y bajo costo.

Sin embargo, el crecimiento de las amenazas cibernéticas y el incremento de la capacidad de procesamiento de los sistemas informáticos han favorecido la aparición de diversas técnicas orientadas a vulnerar los mecanismos de autenticación. Entre ellas, los ataques de fuerza bruta representan una de las estrategias más conocidas y consisten en probar sistemáticamente todas las combinaciones posibles de caracteres hasta determinar la contraseña correcta. El National Institute of Standards and Technology (NIST) define un ataque de fuerza bruta como un procedimiento basado en la prueba exhaustiva de combinaciones alfanuméricas con el propósito de obtener acceso a un dispositivo o sistema protegido [2].

La efectividad de este tipo de ataques ha generado una creciente preocupación en el ámbito de la ciberseguridad, debido a que las credenciales de acceso constituyen uno de los principales objetivos de los ciberdelincuentes. Scarfone y Burr [3] señalan que las amenazas actuales contra las contraseñas han evolucionado considerablemente, por lo que las organizaciones deben implementar políticas de seguridad más robustas y mecanismos complementarios de autenticación para reducir la probabilidad de accesos no autorizados. Asimismo, sostienen que la protección de las credenciales no debe limitarse únicamente a la complejidad de las contraseñas, sino que debe incorporar estrategias adicionales que permitan mitigar los riesgos asociados a los ataques automatizados.

Diversas investigaciones han demostrado que la resistencia de una contraseña frente a un ataque de fuerza bruta depende de varios factores, entre ellos el tamaño del espacio de búsqueda, la longitud y complejidad de la contraseña, la capacidad computacional del atacante y los métodos empleados para almacenar las credenciales. En este sentido, Sahin, Lychev y Wagner [4] sostienen que estos elementos influyen directamente en la dificultad de recuperación de las contraseñas mediante técnicas de búsqueda exhaustiva. Del mismo modo, Yona y Diggavi [5] indican que la utilización de funciones hash y mecanismos criptográficos adecuados incrementa considerablemente la seguridad de los sistemas de autenticación y dificulta la obtención de las credenciales por parte de atacantes.

A pesar de los avances en materia de seguridad informática, los ataques de fuerza bruta continúan representando una amenaza significativa para la protección de la información digital. Esta situación pone de manifiesto la necesidad de comprender el funcionamiento de estas técnicas y de analizar las medidas de seguridad implementadas para contrarrestarlas, con el propósito de fortalecer los mecanismos de autenticación y reducir el riesgo de accesos no autorizados.

En este contexto, el presente artículo tiene como objetivo general analizar la aplicación del método de fuerza bruta en la protección de contraseñas electrónicas, considerando su funcionamiento, los factores que afectan su eficacia y las principales estrategias de seguridad implementadas para prevenir accesos no autorizados. Para ello, se plantea describir el funcionamiento del algoritmo de fuerza bruta y su aplicación en la evaluación de la seguridad de las contraseñas electrónicas; identificar los factores que determinan la vulnerabilidad de las contraseñas frente a este tipo de ataques, tales como la longitud, complejidad y diversidad de caracteres utilizados; estudiar las principales técnicas y mecanismos de protección empleados en los sistemas de autenticación para disminuir la efectividad de los ataques de fuerza bruta; analizar la importancia del uso de contraseñas robustas y de medidas complementarias de seguridad para fortalecer la protección de la información digital; y determinar el impacto que tiene este método en la seguridad informática y en la implementación de políticas de autenticación más seguras.

II. MATERIALES Y METODOS

A. Tipo de Investigación

La presente investigación corresponde a un estudio de carácter documental y descriptivo, orientado al análisis de la aplicación del método de fuerza bruta en la seguridad de contraseñas electrónicas. El trabajo se fundamentó en la recopilación, revisión y análisis de información proveniente de fuentes bibliográficas especializadas relacionadas con la seguridad informática, la criptografía y los mecanismos de autenticación digital.

B. Fuentes de Información

La información empleada en esta investigación fue obtenida a partir de libros, artículos científicos, estándares internacionales y documentos técnicos publicados por organismos y autores reconocidos en el área de la ciberseguridad. Entre las principales fuentes consultadas se encuentran las obras de Stallings [1], Schneier [6], Menezes et al. [7] y Bishop [8], así como las publicaciones del National Institute of Standards and Technology (NIST) [2], [3], las directrices de autenticación digital establecidas en la NIST Special Publication 800-63B [9] y las recomendaciones de seguridad proporcionadas por la Open Worldwide Application Security Project (OWASP) [10].

C. Procedimiento de Investigación

La metodología utilizada se desarrolló en cuatro etapas. En la primera etapa se realizó una búsqueda y recopilación de información relacionada con los mecanismos de autenticación y los ataques de fuerza bruta. Posteriormente, se efectuó una revisión de la literatura especializada con el propósito de identificar los principales conceptos, características y factores asociados con la vulnerabilidad de las contraseñas electrónicas.

En una tercera etapa se analizaron las investigaciones y documentos técnicos referentes a los mecanismos de protección implementados en los sistemas modernos de autenticación, tales como las funciones hash, el uso de salting, la autenticación multifactor y las políticas de complejidad de contraseñas. Finalmente, se compararon las diferentes estrategias de seguridad descritas en la literatura con el fin de evaluar su contribución en la mitigación de ataques de fuerza bruta y en el fortalecimiento de la protección de las credenciales digitales.

D. Método de Análisis

El análisis de la información se realizó mediante una revisión bibliográfica sistemática y un enfoque comparativo. Para ello, se clasificaron las fuentes consultadas de acuerdo con su contribución al estudio, considerando aspectos relacionados con el funcionamiento del algoritmo de fuerza bruta, los factores que influyen en su efectividad y las principales medidas de seguridad empleadas para contrarrestar este tipo de ataques.

La información recopilada fue organizada y analizada con el propósito de establecer una visión integral sobre la influencia del método de fuerza bruta en la seguridad informática y sobre la importancia de implementar mecanismos de autenticación robustos para la protección de la información digital.

III. RESULTADOS

A. Funcionamiento del Método de Fuerza Bruta

El análisis realizado permitió identificar que el método de fuerza bruta consiste en un procedimiento de búsqueda exhaustiva mediante el cual se prueban sistemáticamente todas las combinaciones posibles de caracteres hasta encontrar la contraseña correcta. El número de combinaciones generadas depende directamente del conjunto de caracteres disponibles y de la longitud de la contraseña.

$$N = C^L$$

- C: Corresponde al número de caracteres disponibles.
- L: Representa la longitud de la contraseña.
- N: Representa el número total de combinaciones posibles.

La cantidad total de combinaciones posibles puede expresarse mediante la ecuación:

Se observó que el incremento en la longitud de la contraseña produce un crecimiento exponencial del espacio de búsqueda, aumentando el tiempo necesario para completar un ataque de fuerza bruta.

B. Factores que Influyen en la Vulnerabilidad de las Contraseñas

Los resultados obtenidos permitieron establecer que la vulnerabilidad de una contraseña está determinada principalmente por su longitud, la diversidad de caracteres empleados y la capacidad computacional disponible para realizar el ataque.

Las contraseñas cortas y conformadas únicamente por números o letras presentaron un menor número de combinaciones posibles, mientras que aquellas que incorporan letras mayúsculas, minúsculas, números y caracteres especiales incrementan significativamente la complejidad del proceso de búsqueda.

La Tabla I presenta una clasificación general del nivel de seguridad de las contraseñas según sus características.

TABLA I

CLASIFICACIÓN DE NIVEL DE SEGURIDAD

Longitud	Tipo de caracteres	Nivel de seguridad
6 caracteres	Solo números	Muy bajo
8 caracteres	Letras y números	Bajo
10 caracteres	Letras mayúsculas, minúsculas y números	Medio
12 caracteres	Letras, números y símbolos especiales	Alto
16 o más caracteres	Combinación completa de caracteres	Muy alto

C. Principales Mecanismos y Algoritmos de Protección

Los resultados obtenidos permitieron identificar diversos mecanismos y algoritmos empleados para disminuir la efectividad de los ataques de fuerza bruta y fortalecer la seguridad de los sistemas de autenticación. Entre los principales se encontraron:

- Funciones hash.
- Salting.
- Autenticación multifactor.
- CAPTCHA.
- Limitación del número de intentos.
- Bloqueo temporal de cuentas.
- Gestores de contraseñas.

D. Algoritmos Utilizados para el Almacenamiento Seguro de Contraseñas

TABLA II

ALGORITMOS PARA GUARDADO DE CONTRASEÑAS

Algoritmo	Nivel de seguridad	Uso actual
MD5	Bajo	Obsoleto
SHA-1	Bajo	Desaconsejado
SHA-256	Alto	Recomendado
PBKDF2	Alto	Amplio uso
bcrypt	Muy Alto	Muy recomendado
Scrypt	Muy Alto	Amplio uso
Argon2	Excelente	Estado de arte

IV. DISCUSIÓN

Los resultados obtenidos permitieron confirmar que el método de fuerza bruta continúa representando una de las técnicas más utilizadas para comprometer sistemas de autenticación basados en contraseñas. El análisis realizado evidenció que la efectividad de este tipo de ataques depende principalmente del tamaño del espacio de búsqueda, de la longitud de las contraseñas y de la diversidad de caracteres empleados, lo cual coincide con lo planteado por Sahin, Lychev y Wagner [4], quienes sostienen que la complejidad de las contraseñas influye directamente en la dificultad para recuperarlas mediante técnicas de búsqueda exhaustiva.

Asimismo, los resultados mostraron que las contraseñas conformadas únicamente por caracteres numéricos o con una longitud reducida presentan un menor nivel de seguridad frente a ataques automatizados. Este comportamiento respalda las recomendaciones establecidas por Stallings [1], quien señala que la fortaleza de los mecanismos de autenticación depende en gran medida de la complejidad y robustez de las credenciales utilizadas por los usuarios.

Por otra parte, el estudio permitió identificar que los mecanismos tradicionales de protección basados exclusivamente en contraseñas resultan insuficientes frente al incremento de la capacidad computacional y al uso de herramientas automatizadas capaces de ejecutar millones de intentos por segundo. En este sentido, los resultados obtenidos concuerdan con las observaciones realizadas por Scarfone y Burr [3], quienes indican que la seguridad de las credenciales no debe depender únicamente de la complejidad de las contraseñas, sino complementarse con políticas de autenticación más robustas y mecanismos adicionales de protección.

De igual manera, la comparación entre diferentes algoritmos utilizados para el almacenamiento seguro de contraseñas evidenció diferencias significativas en sus niveles de seguridad. Los algoritmos MD5 y SHA-1 presentaron limitaciones debido a las vulnerabilidades conocidas y a la existencia de métodos que permiten comprometer su integridad. En contraste, algoritmos como PBKDF2, bcrypt, scrypt y Argon2 mostraron una mayor resistencia frente a ataques de fuerza bruta gracias a la incorporación de funciones de derivación de claves y al incremento del costo computacional requerido para recuperar las credenciales. Estos resultados son consistentes con las investigaciones desarrolladas por Yona y Diggavi [5], quienes destacan la importancia de los mecanismos criptográficos en la protección de la información.

Además, se observó que la implementación de estrategias complementarias, tales como el uso de salting, la autenticación multifactor, la limitación del número de intentos de acceso y los bloqueos temporales de cuentas, contribuyen significativamente a disminuir la efectividad de los ataques de fuerza bruta. Estas medidas coinciden con las recomendaciones propuestas por el National Institute of Standards and Technology (NIST) y por la Open Worldwide Application Security Project (OWASP), las cuales establecen la necesidad de adoptar enfoques de seguridad multicapa para reducir el riesgo de accesos no autorizados.

Finalmente, los resultados obtenidos permitieron evidenciar que el estudio del método de fuerza bruta no solamente resulta relevante para comprender las vulnerabilidades presentes en los sistemas de autenticación, sino también para promover el diseño de políticas de seguridad más eficientes y fortalecer la protección de la información digital. En consecuencia, la implementación de contraseñas robustas y de mecanismos adicionales de autenticación constituye un elemento esencial para enfrentar las amenazas cibernéticas en entornos digitales cada vez más complejos y dinámicos.

V. CONCLUSIÓN

El análisis realizado permitió establecer que el método de fuerza bruta constituye una técnica de búsqueda exhaustiva cuya efectividad depende principalmente de la longitud y complejidad de las contraseñas, así como de la capacidad computacional disponible para ejecutar los ataques. En consecuencia, las contraseñas simples y de reducido tamaño presentan una mayor vulnerabilidad frente a este tipo de amenazas.

La investigación evidenció que la implementación de mecanismos complementarios de seguridad, tales como las funciones hash, el uso de salting, la autenticación multifactor y las políticas de restricción de intentos de acceso, contribuyen significativamente a disminuir la efectividad de los ataques de fuerza bruta y a fortalecer los sistemas de autenticación modernos.

Asimismo, se determinó que algoritmos especializados para el almacenamiento seguro de contraseñas, como bcrypt, PBKDF2, scrypt y Argon2, ofrecen mayores niveles de protección en comparación con algoritmos tradicionales como MD5 y SHA-1, debido a su mayor resistencia frente a ataques de búsqueda exhaustiva y a la incorporación de mecanismos adicionales de seguridad.

Los resultados obtenidos permitieron confirmar la importancia de promover el uso de contraseñas robustas y de adoptar estrategias de seguridad multicapa con el fin de proteger la información digital y reducir la probabilidad de accesos no autorizados. De esta manera, el estudio contribuye a una mejor comprensión del impacto del método de fuerza bruta en la seguridad informática y resalta la necesidad de implementar políticas de autenticación más seguras en entornos digitales cada vez más expuestos a amenazas cibernéticas.

Finalmente, como trabajo futuro, se propone profundizar en el estudio de técnicas avanzadas de protección de credenciales, así como analizar la influencia de tecnologías emergentes, tales como la inteligencia artificial, la computación cuántica y los sistemas de autenticación sin contraseñas, con el propósito de desarrollar mecanismos de seguridad capaces de responder a los nuevos desafíos presentes en el ámbito de la ciberseguridad.

VI. RECONOCIMIENTOS

Los autores expresan su agradecimiento a los docentes y a la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Trujillo por los conocimientos y orientaciones brindadas durante el desarrollo de la presente investigación. Asimismo, se reconoce el aporte de las diferentes fuentes bibliográficas, organismos especializados y comunidades científicas relacionadas con la seguridad informática y la ciberseguridad, cuya información permitió sustentar el análisis realizado.

De igual manera, se agradece a todas las personas que, mediante sus observaciones y recomendaciones, contribuyeron al fortalecimiento y mejora del presente trabajo de investigación.

VI. REFERENCIAS BIBLIOGRÁFICAS

[1]. W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Boston, MA, USA: Pearson, 2017.

[2]. National Institute of Standards and Technology (NIST), Glossary: Brute Force Password Attack. Gaithersburg, MD, USA: NIST, 2024. [Online]. Available: https://csrc.nist.gov/glossary/term/brute_force_password_attack

[3]. K. Scarfone and W. Burr, Guide to Enterprise Password Management (Draft), National Institute of Standards and Technology, Gaithersburg, MD, USA, Special Publication 800-118, 2009.

[4]. C. S. Sahin, R. Lychev, and N. Wagner, “General Framework for Evaluating Password Complexity and Strength,” arXiv preprint arXiv:1512.05814, Dec. 2015. [Online]. Available: https://arxiv.org/abs/1512.05814

[5]. Y. Yona and S. Diggavi, “The Guesswork of Hash Functions,” arXiv preprint arXiv:1608.02132, Aug. 2016.

[6]. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York, NY, USA: John Wiley & Sons, 1996.

[7]. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.

[8]. M. Bishop, Computer Security: Art and Science, 2nd ed. Boston, MA, USA: Addison-Wesley, 2018.

[9]. National Institute of Standards and Technology, Digital Identity Guidelines: Authentication and Lifecycle Management, NIST Special Publication 800-63B, Gaithersburg, MD, USA, 2020.

[10]. OWASP Foundation, Authentication Cheat Sheet, 2024. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html