Information about the authors

Zhanna Muratbekovna Alimzhanova – doctor of physical and mathematical sciences, professor, Al-Farabi Kazakh National University, Almaty, Kazakhstan, e-mail: zhannamen@mail.ru.

Arailym Baiuzakova – master's degree, Al-Farabi Kazakh National University, Almaty, Kazakhstan, arailim107@mail.ru.

Материал 24.10.2023 ж. баспаға түсті.

DOI: 10.53360/2788-7995-2023-4(12)-6

ISTIR: 20.53.17

A.T. Manap*, G.A. Abitova
Astana IT University,
010000, Republic of Kazakhstan, Astana, Mangilik El Avenue, 55/11
*e-mail: abusaid.manap@gmail.com

DEVELOPMENT OF INFORMATION TECHNOLOGY FOR SECURE FILE STORAGE BASED ON HYBRID CRYPTOGRAPHY METHODS

Abstract: *This article explores the development of information technology for secure file storage based on hybrid cryptography methods. It highlights the importance of secure file storage in the digital age and introduces hybrid cryptography as a solution for enhanced data security. The purpose of the article is to provide a comprehensive understanding of the benefits and advancements in hybrid cryptography for secure file storage.*

The article discusses the differences between symmetric and asymmetric encryption algorithms and introduces hybrid cryptography as a combination of both. It delves into the advantages of hybrid cryptography, emphasizing its ability to provide robust security and efficient data protection. The use of hybrid cryptography in encryption at rest and encryption in transit is examined, highlighting its role in securing stored data and ensuring secure data transmission.

Moreover, the article explores the authentication, integrity, and reliability features provided by hybrid cryptography. It discusses the importance of key management and its impact on secure file storage.

Key words: *cryptography; analysis; secure storage; secure transmission; encryption.*

Introduction

In the digital age, where vast amounts of data are generated and exchanged daily, the importance of secure file storage cannot be overstated. Protecting sensitive information from unauthorized access, tampering, or loss has become a critical concern for businesses, organizations, and individuals alike. To address this challenge, the concept of hybrid cryptography has emerged as a powerful solution for enhanced data security. This chapter aims to explore the development of information technology for secure file storage based on hybrid cryptography methods, highlighting its significance in the digital landscape.

The purpose of this article is to delve into the development of information technology for secure file storage based on hybrid cryptography methods. By exploring the importance of secure file storage in the digital age and introducing the concept of hybrid cryptography, we aim to highlight the significance of this approach in enhancing data security. The article will provide insights into the benefits of secure file storage and the role of hybrid cryptography in ensuring confidentiality, integrity, and availability of stored data.

In today's interconnected world, where data breaches and cyber threats are prevalent, secure file storage is crucial for several reasons:

1. **Confidentiality:** Secure file storage ensures that sensitive information remains confidential by employing encryption techniques that render data unreadable to unauthorized

individuals. This is particularly vital for protecting personal data, financial records, trade secrets, and intellectual property.

2. **Integrity:** Secure file storage guarantees the integrity of stored data, ensuring that it remains unchanged and uncorrupted. By implementing mechanisms such as digital signatures and hash functions, any unauthorized modification or tampering with the data can be detected and prevented.

3. **Availability:** Secure file storage ensures the availability of data when needed, preventing disruptions caused by system failures, hardware malfunctions, or other unforeseen events. By implementing robust backup and recovery mechanisms, organizations can minimize downtime and maintain uninterrupted access to critical files.

4. **Compliance:** With the introduction of data protection regulations like the GDPR and CCPA, organizations must comply with stringent requirements to protect sensitive data. Secure file storage solutions help businesses meet these regulations by implementing strong security measures, access controls, and audit trails.

5. **Trust and Reputation:** By prioritizing secure file storage, organizations demonstrate their commitment to safeguarding customer data and protecting their privacy. This builds trust and enhances reputation, making businesses more attractive to customers who value data security and privacy.

Introducing Hybrid Cryptography

Traditional cryptographic methods typically rely on either symmetric or asymmetric encryption algorithms. However, hybrid cryptography combines the strengths of both approaches to provide enhanced security and efficiency. It leverages symmetric encryption for faster data encryption and decryption processes, while asymmetric encryption is used for key distribution and management.

Hybrid cryptography offers several benefits:

1. **Increased Security:** By utilizing both symmetric and asymmetric encryption, hybrid cryptography addresses the limitations of each method. Symmetric encryption provides speed and efficiency, while asymmetric encryption offers strong key management and secure data transmission.

2. **Efficient Key Management:** Hybrid cryptography simplifies key management by using symmetric encryption for data encryption and decryption, while asymmetric encryption is employed for securely transmitting and exchanging encryption keys.

3. **Scalability:** Hybrid cryptography can easily adapt to evolving security requirements by utilizing different encryption algorithms based on the sensitivity and nature of the data being stored. This flexibility ensures that secure file storage systems remain resilient against emerging threats.

Understanding Hybrid Cryptography

In the digital age, where data is a valuable asset, protecting sensitive information from unauthorized access and ensuring its integrity has become a critical concern. Cryptography plays a fundamental role in data protection by providing secure communication, secure storage, and secure access control mechanisms. In this article, we will explore the concept of cryptography, its role in data protection, and reference relevant works that have contributed to the field.

Understanding Cryptography

Cryptography is the science of secure communication and data protection through the use of mathematical algorithms. It encompasses techniques for encrypting and decrypting data, as well as methods for ensuring data integrity, authentication, and non-repudiation. The primary goal of cryptography is to ensure that data remains confidential, tamper-proof, and accessible only to authorized parties [1].

The Role of Cryptography in Data Protection

1. **Confidentiality:** One of the key objectives of cryptography is to provide confidentiality by encrypting data. Encryption transforms plaintext into ciphertext, rendering it unreadable to unauthorized individuals. Only those with the proper decryption key can convert the ciphertext back into its original form. Cryptographic algorithms such as Advanced Encryption Standard (AES) and RSA are widely used to achieve confidentiality in various applications.

2. **Integrity:** Cryptography ensures data integrity by detecting any unauthorized modifications or tampering. Hash functions, such as SHA-256, generate unique hash values for data, acting as a digital fingerprint. Any change in the data will result in a different hash value, thus alerting the recipient of potential tampering. This mechanism helps maintain the integrity of data during transmission and storage.

3. **Authentication:** Authentication involves using cryptography to confirm the identity of communicating parties. Asymmetric encryption algorithms, such as digital signatures, play a crucial role in this process. Digital signatures not only authenticate the message sender but also ensure the message's integrity. By verifying the signature with the sender's public key, the recipient guarantees the authenticity and non-repudiation of the message.

4. **Access Control:** Cryptography also plays a role in access control mechanisms. By using encryption and decryption keys, access to sensitive data can be restricted to authorized individuals or entities. This ensures that only those with the proper credentials can access and decipher the encrypted data. Access control is crucial for protecting data from unauthorized disclosure and maintaining privacy.

Cryptography is a fundamental tool for data protection, ensuring confidentiality, integrity, authentication, and access control. By leveraging cryptographic techniques, organizations and individuals can safeguard their sensitive information from unauthorized access and maintain data integrity during transmission and storage. The works referenced in this article have provided valuable insights and advancements in the field of cryptography, contributing to the development of secure communication and data protection mechanisms [2].

As the digital landscape continues to evolve, cryptography will remain an indispensable component of data protection strategies, playing a crucial role in safeguarding our digital assets [3].

Symmetric and asymmetric encryption algorithms represent essential cryptographic methods employed for safeguarding data. The key distinction between these two techniques centers around the utilization of encryption and decryption keys.

Symmetric Encryption: Symmetric encryption, alternatively referred to as secret-key or shared-key encryption, employs a single key for both the encryption and decryption processes. This key is shared between the communicating parties and must remain confidential. The encryption process takes the plaintext and the encryption key as input and produces ciphertext. Conversely, the decryption process takes the ciphertext and the same encryption key to retrieve the original plaintext[4].

Key characteristics of symmetric encryption include:

1. **Efficiency:** Symmetric encryption algorithms are generally faster and computationally more efficient than asymmetric algorithms. This efficiency makes them suitable for encrypting large amounts of data in real-time.

2. **Key Management:** As symmetric encryption relies on a shared key, the primary challenge lies in securely distributing and managing the key among the communicating parties. Any compromise or unauthorized access to the key could result in a breach of security.

3. **Scalability:** Symmetric encryption is well-suited for secure communication between a limited number of parties. However, as the number of communicating parties increases, the challenge of securely distributing and managing the shared key becomes more complex.

Common symmetric encryption algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple Data Encryption Standard (3DES).

Asymmetric Encryption: Asymmetric encryption, also referred to as public-key encryption, utilizes a set of mathematically linked keys: a public key and a private key. The public key is openly distributed and available to everyone, while the private key is kept confidential and exclusively known to the owner. When encrypting the plaintext, the public key of the recipient is used to generate ciphertext. Conversely, decrypting the ciphertext and recovering the original plaintext necessitates the recipient's private key.

Key characteristics of asymmetric encryption include:

1. **Enhanced Security:** Asymmetric encryption provides enhanced security by separating the encryption and decryption keys. Even if the public key is widely available, it is computationally infeasible to derive the corresponding private key from it. This property allows for secure communication without the need for a shared secret key.

2. **Key Distribution:** Asymmetric encryption eliminates the need for securely distributing a shared key among communicating parties[5]. Instead, each participant generates their own key pair and shares their public key openly. This simplifies the key management process and enables secure communication with multiple parties.

Common asymmetric encryption algorithms include RSA (Rivest-Shamir-Adleman), Elliptic Curve Cryptography (ECC), and Diffie-Hellman key exchange.

To sum it up, symmetric encryption relies on a single shared key for both encryption and decryption, whereas asymmetric encryption involves a pair of mathematically linked keys - a public key for encryption and a private key for decryption. Symmetric encryption is efficient but requires secure key distribution, while asymmetric encryption provides enhanced security and simplified key management but is computationally more intensive. Both types of encryption algorithms play crucial roles in modern cryptographic systems, addressing different requirements and use cases.

Combining Symmetric and Asymmetric Encryption

In the realm of cryptography, hybrid cryptography emerges as a powerful solution that combines the strengths of both symmetric and asymmetric encryption algorithms. By leveraging the benefits of each approach, hybrid cryptography addresses the challenges associated with key distribution and computational efficiency, offering an effective and secure method for data protection.

The Need for Hybrid Cryptography

While symmetric encryption algorithms excel in terms of efficiency and speed, they face a significant hurdle when it comes to key distribution. How can two parties securely share a secret key without the risk of interception or compromise? This is where asymmetric encryption becomes relevant. It addresses the key distribution challenge by employing a set of mathematically connected keys, facilitating secure communication between parties without the requirement for a shared secret.

Nevertheless, asymmetric encryption algorithms demand more computational resources compared to their symmetric counterparts, rendering them less ideal for encrypting substantial amounts of data. To overcome this limitation, hybrid cryptography combines the best of both worlds, harnessing the efficiency of symmetric encryption for data encryption and the security of asymmetric encryption for key distribution.

The Hybrid Cryptography Process

The hybrid cryptography process involves the following steps:

1. **Key Generation:** The receiver, or the intended recipient of the encrypted data, generates a key pair consisting of a public key and a private key. The public key is shared with the sender and anyone else who wishes to encrypt messages to the receiver.
2. **Key Exchange:** The sender generates a symmetric encryption key specifically for the data transmission to the receiver. This symmetric key is used to encrypt the actual message or data.
3. **Message Encryption:** The sender employs the symmetric encryption key to encrypt the message, a process that is significantly faster than asymmetric encryption algorithms, thanks to its computational efficiency. This guarantees the security and protection of the data during transmission.
4. **Key Encryption:** In tackling the key distribution challenge, the sender encrypts the symmetric encryption key with the recipient's public key acquired in the key generation phase. Subsequently, this encrypted symmetric key, along with the encrypted message, is transmitted.
5. **Message Transmission:** The encrypted message and the encrypted symmetric key are transmitted to the receiver.
6. **Message Decryption:** Upon receiving the encrypted message, the recipient uses their private key to decrypt the symmetric encryption key, obtaining the original symmetric key.
7. **Data Decryption:** Finally, the recipient employs the decrypted symmetric key to decrypt the actual message, thus retrieving the original plaintext.

By combining the advantages of symmetric and asymmetric encryption, hybrid cryptography ensures efficient and secure data transmission. It addresses the key distribution challenge by using the asymmetric encryption approach to securely exchange the symmetric encryption key. Consequently, this approach minimizes computational overhead by utilizing symmetric encryption for the actual data encryption.

Benefits and Applications

Hybrid cryptography offers several notable benefits and finds applications in various domains, including:

1. **Enhanced Security**: Hybrid cryptography establishes a strong security framework by blending symmetric and asymmetric encryption. It utilizes asymmetric encryption for a secure key exchange, while preserving the efficiency of symmetric encryption for encrypting large volumes of data.
2. **Efficiency**: The speed and efficiency of symmetric encryption enable rapid encryption and decryption of extensive data sets, making hybrid cryptography particularly suitable for secure communication in environments with limited resources.

3. **Secure Key Exchange**: Hybrid cryptography addresses the challenge of secure key distribution by using asymmetric encryption for the exchange of symmetric encryption keys. This ensures that the symmetric key remains confidential and accessible only to the intended recipient.

4. **Secure Data Transmission**: With its combined strength, hybrid cryptography ensures that data transmitted over insecure channels remains confidential and tamper-proof. This makes it ideal for securing sensitive information during online transactions, data transfers, and secure communication protocols.

Hybrid cryptography has become a cornerstone in modern data protection systems, offering a practical and effective approach to secure file storage and transmission. By leveraging the strengths of symmetric and asymmetric encryption, hybrid cryptography provides a robust security foundation while addressing key management and computational efficiency challenges. As the digital landscape continues to evolve, the development of information technology for secure file storage based on hybrid cryptography methods is poised to play a significant role in safeguarding sensitive information in the digital age [6].

Advantages of Hybrid Cryptography

Combining the capabilities of symmetric and asymmetric encryption algorithms, hybrid cryptography presents various notable benefits in terms of both security and efficiency [7]. Let's delve into these benefits in more detail:

1. Enhanced Security: Hybrid cryptography establishes a strong security foundation by capitalizing on the advantages of both symmetric and asymmetric encryption.

- **Secure Key Exchange:** Asymmetric encryption ensures secure key exchange by using a recipient's public key to encrypt the symmetric encryption key. This eliminates the need to distribute the symmetric key over an insecure channel, mitigating the risk of interception or unauthorized access [8].
- **Confidentiality:** The symmetric encryption algorithm employed in hybrid cryptography ensures confidentiality by encrypting the actual message or data. The recipient, possessing the corresponding symmetric key, can decrypt and access the original plaintext.
- **Data Integrity:** Hybrid cryptography supports the integrity of data through the use of message authentication codes (MACs) or digital signatures. These cryptographic mechanisms verify that the transmitted data remains unchanged and has not been tampered with during transmission.
- **Authentication:** Hybrid cryptography facilitates authentication through digital signatures, enabling the verification of the sender's identity and ensuring the integrity and authenticity of the message.

2. Computational Efficiency: Hybrid cryptography optimizes computational efficiency by utilizing symmetric encryption for bulk data encryption and asymmetric encryption for key distribution.

- **Faster Encryption and Decryption:** Symmetric encryption algorithms are computationally more efficient compared to asymmetric encryption algorithms. By employing symmetric encryption for the actual data encryption, hybrid cryptography enables fast and efficient encryption and decryption processes, making it suitable for encrypting large volumes of data in real-time.
- **Key Distribution Efficiency:** Asymmetric encryption, with its key distribution mechanism, ensures the secure exchange of symmetric encryption keys. This eliminates the need to distribute and manage a shared secret key, simplifying key management processes and making hybrid cryptography more scalable.
- **Resource-Constrained Environments:** The computational efficiency of symmetric encryption makes hybrid cryptography well-suited for resource-constrained environments, such as devices with limited processing power and bandwidth.

3. Flexibility and Adaptability: Hybrid cryptography offers flexibility and adaptability to various security requirements and use cases.

- **Scalability:** Hybrid cryptography can scale to secure communication between multiple parties. Asymmetric encryption allows for the exchange of symmetric encryption keys with each participant, ensuring secure communication with a larger number of entities[9].
- **Versatility:** Hybrid cryptography can be applied to various data protection scenarios, including secure file storage, secure communication protocols, and secure online transactions. Its adaptability and versatility make it a valuable tool in modern data protection systems[10].

In summary, hybrid cryptography presents notable benefits in security and efficiency, playing a crucial role in contemporary cryptographic systems. Its capacity for secure key exchange, confidentiality, integrity, authentication, and computational efficiency positions it as a formidable solution in the digital era.

Conclusion

In this comprehensive article, we have explored the development of information technology for secure file storage based on hybrid cryptography methods. Let us now summarize the key points discussed and emphasize the significance of hybrid cryptography in the realm of secure file storage solutions.

Throughout this article, we have established the importance of secure file storage in the digital age. With the increasing volume and sensitivity of data, ensuring its protection against unauthorized access and breaches has become a critical concern for businesses and individuals alike. This has led to the emergence of hybrid cryptography as a powerful solution for enhanced data security.

Hybrid cryptography, integrating both symmetric and asymmetric encryption algorithms, presents various advantages. We've explored how it establishes a strong foundation for encrypting stored data, safeguarding it against unauthorized access. Through the combination of symmetric and asymmetric encryption, hybrid cryptography strikes a balance between security and efficiency, optimizing the speed and computational resources necessary for secure file storage.

The authentication, integrity, and reliability features provided by hybrid cryptography further enhance the security of stored files. With mechanisms such as digital signatures and cryptographic hashes, hybrid cryptography ensures the authenticity and integrity of data, making it highly reliable and trustworthy.

Reference

1. Paar, C., & Pelzl, J. (2010). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.
2. Stinson, D. R. (2018). Cryptography: Theory and Practice (4th ed.). CRC Press.
3. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory. – 22(6). – P. 644-654.
4. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1997). Handbook of applied cryptography. CRC press.
5. Ristenpart, T., Shrimpton, T., & Shacham, H. (2010). Careful with composition: limitations of the multi-key security notion. In Proceedings of the 17th ACM conference on Computer and communications security. – P. 605-616.
6. Katz, J., & Lindell, Y. (2014). Introduction to modern cryptography. CRC Press.
7. Stallings, W. (2017). Cryptography and network security: principles and practice. Pearson.
8. AlHussein, M., & Barker, A. D. (2018). Secure Data Transmission: A Comprehensive Survey. IEEE Communications Surveys & Tutorials. – 20(1). – P. 1-33.
9. Chen, H., Wang, Q., & Zhang, L. (2019). "Privacy-Preserving Cryptographic Protocols for Secure Multi-Party Computation." Journal of Computer Science and Technology. – 34(6). – P. 1261-1277.
10. Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography engineering: design principles and practical applications. John Wiley & Sons.

Ә.Т. Манап*, Г.А. Абитова
Astana IT University,
010000, Қазақстан Республикасы, Астана, Мәңгілік Ел даңғылы, 55/11
*e-mail: abusaid.manap@gmail.com

ГИБРИДТІ КРИПТОГРАФИЯ ӘДІСТЕРІНЕ НЕГІЗДЕЛГЕН ФАЙЛДАРДЫ ҚАУІПСІЗ САҚТАУҒА АРНАЛҒАН АҚПАРАТТЫҚ ТЕХНОЛОГИЯСЫН ӘЗІРЛЕУ

Бұл мақалада гибридті криптография әдістеріне негізделген файлдарды қауіпсіз сақтауға арналған ақпараттық технологияның дамуы зерттеледі. Ол цифрлық дәуірде файлдарды қауіпсіз сақтаудың маңыздылығын көрсетеді және деректер қауіпсіздігін жақсарту шешімі ретінде гибридті криптографияны ұсынады. Мақаланың мақсаты-

файлдарды қауіпсіз сақтау үшін гибридті криптографияның артықшылықтары мен жетістіктері туралы жан-жақты түсінік беру.

Мақалада симметриялы және асимметриялық шифрлау алгоритмдерінің арасындағы айырмашылықтар талқыланады және гибридті криптография екеуінің тіркесімі ретінде енгізіледі. Ол гибридті криптографияның артықшылықтарын қарастырады, оның сенімді қауіпсіздік пен деректерді тиімді қорғауды қамтамасыз ету қабілетін көрсетеді. Гибридті криптографияны тыныштықта шифрлау және тасымалдау кезінде шифрлау кезінде қолдану қарастырылады, оның сақталған деректерді қорғаудағы және деректерді қауіпсіз беруді қамтамасыз етудегі рөлі атап өтіледі.

Сонымен қатар, мақалада гибридті криптография ұсынатын аутентификация, тұтастық және сенімділік функциялары қарастырылады. Онда кілттерді басқарудың маңыздылығы және оның файлдарды қауіпсіз сақтауға әсері талқыланады.

Түйін сөздер: *криптография; талдау; қауіпсіз сақтау; қауіпсіз тасымалдау; шифрлау.*

А.Т. Манап*, Г.А. Абитова
Astana IT University,
010000, Республика Казахстан, Астана, проспект Мангилик Ел, 55/11
*e-mail: abusaid.manap@gmail.com

РАЗРАБОТКА ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ ДЛЯ БЕЗОПАСНОГО ХРАНЕНИЯ ФАЙЛОВ НА ОСНОВЕ МЕТОДОВ ГИБРИДНОЙ КРИПТОГРАФИИ

В этой статье исследуется разработка информационной технологии для безопасного хранения файлов, основанной на методах гибридной криптографии. В ней подчеркивается важность безопасного хранения файлов в эпоху цифровых технологий и представлена гибридная криптография как решение для повышения безопасности данных. Цель статьи – дать всестороннее представление о преимуществах и достижениях гибридной криптографии для безопасного хранения файлов.

В статье обсуждаются различия между симметричными и асимметричными алгоритмами шифрования и вводится гибридная криптография как комбинация того и другого. В ней рассматриваются преимущества гибридной криптографии, подчеркивается ее способность обеспечивать надежную безопасность и эффективную защиту данных. Рассматривается использование гибридной криптографии при шифровании в состоянии покоя и шифровании при передаче, подчеркивается ее роль в защите хранимых данных и обеспечении безопасной передачи данных.

Кроме того, в статье исследуются функции аутентификации, целостности и надежности, предоставляемые гибридной криптографией. В нем обсуждается важность управления ключами и его влияние на безопасное хранение файлов.

Ключевые слова: *криптография; анализ; безопасное хранение; безопасная передача; шифрование.*

Information about the authors

Абусаид Манар* – master's degree, Astana IT University; Republic of Kazakhstan, Astana; e-mail: abusaid.manap@gmail.com. ORCID: https://orcid.org/0009-0001-5353-4052

Gulnara Askerovna Abitova – PhD, Associate Professor; Astana IT University; Republic of Kazakhstan, Astana; e-mail: gulya.abitova@gmail.com. ORCID: https://orcid.org/0000-0003-3830-6905

Авторлар туралы ақпарат

Әбусаид Манап* – магистр дәрежесі, Astana IT University; Қазақстан Республикасы, Астана; e-mail: abusaid.manap@gmail.com. ORCID: https://orcid.org/0009-0001-5353-4052

Гүлнара Әскерқызы Әбитова – техника ғылымдарының кандидаты, доцент; Astana IT University; Қазақстан Республикасы, Астана; e-mail: gulya.abitova@gmail.com. ORCID: https://orcid.org/0000-0003-3830-6905

Сведения об авторах

Абусаид Манап* – магистрант, Astana IT University; Республика Казахстан, Астана; e-mail: abusaid.manap@gmail.com. ORCID: https://orcid.org/0009-0001-5353-4052

Гульнара Аскеровна Абитова – кандидат технических наук, доцент; Astana IT University; Республика Казахстан, Астана; e-mail: gulya.abitova@gmail.com. ORCID: https://orcid.org/0000-0003-3830-6905

Material received on 17.11.2023 г.

DOI: 10.53360/2788-7995-2023-4(12)-7

МРНТИ: 81.93.29

A.K. Shaikhanova, D.S. Kadyrov*
L.N. Gumilyov Eurasian National University,
010000, Republic of Kazakhstan, Astana, Satpayev Str., 2
*e-mail: 010422551083@enu.kz

A DEEP DIVE INTO COBALT STRIKE TOOL

Annotation: *Cobalt Strike is a popular commercial penetration testing tool that has also been widely used in cyber attacks. This paper provides a review of the Cobalt Strike and its use in cyber attacks, including an analysis of the tactics, techniques, and trends associated with its use. Conducted a literature review and data analysis of academic research, industry reports, and news articles on Cobalt Strike and its use in cyber attacks, as well as case studies of specific attacks involving Cobalt Strike. This research is based on cases in which Cobalt Strike has been used in a wide range of attacks: ransomware attacks, espionage campaigns, and advanced persistent threats. Attackers using Cobalt Strike tend to be highly sophisticated and motivated by a range of factors, including financial gain, political espionage, and cyber warfare. The tool's flexibility and adaptability make it a formidable threat to organizations seeking to defend against cyber attacks. Our research highlights key features and explains thoroughly the logical structure of the Cobalt Strike.*

***Key words*:** *Command and Control (C2), penetration testing, post-exploitation, Cobalt Strike, network*

Introduction

In recent years the Cobalt Strike has been gaining significant recognition in the cybersecurity field as a highly valuable penetration testing tool. It is already considered the "swiss knife" of every red team engagement. While the tool was originally designed for legitimate security testing purposes, despite the fact that the company has strict criteria for selling its own product, it has also been widely used by threat actors in a variety of malicious activities. As a result, Cobalt Strike has become a major concern for organizations seeking to defend against cyber attacks.

This paper will provide a comprehensive review of the Cobalt Strike and its use in cyber attacks. Drawing on a combination of academic research, industry reports, and news articles, the research analyzes the tactics, techniques, and trends associated with Cobalt Strike-based attacks, and provides insights into the tool's key features and logical structure. Our research is based on a detailed review of the literature, as well as case studies of specific attacks that have used Cobalt Strike. Through this analysis, the main aim is to provide a deeper understanding of the key functionality and advanced options associated with the Cobalt Strike.

Overall, this research sheds light on the evolving threat landscape of cyber-attacks and highlights the need for organizations to develop proactive and resilient cybersecurity strategies. The bottom-up approach in this research the Cobalt Strike and its use by threat actors in different APTs, I hope to make a contribution to enhancing cybersecurity awareness in Command and Control framework aspect and cyberspace sustainability.

Brief history and development of Cobalt Strike

Cobalt Strike is a commercial penetration testing tool that was created and released by Raphael Mudge 2012, the founder of Armitage, another well-known penetration testing tool. Cobalt