Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 6, No. 1, 2023

Research on Vulnerabilities in Computer Information Technology and Encryption Techniques

Zhenan Tu

Biaoliang Technology (Shanghai) Co., Ltd.; Shanghai 200441, China

Abstract: In this era of information, the rapid advancement of computer information technology has brought about tremendous changes to our work and life. However, accompanying this progress are significant challenges in terms of data security. Vulnerabilities in data security and encryption technologies have become the focal point of research, aiming to ensure the utmost protection and security of our data. The purpose of this article is to delve into the vulnerabilities in data security and encryption technologies within the realm of computer information technology, with the intention of providing readers with a profound understanding of data security issues and effective solutions. By comprehensively understanding the origins and impacts of data security vulnerabilities, as well as the principles and applications of encryption technologies, we can become more acutely aware of the importance of data security, enhance our capabilities in safeguarding data security, and contribute to the construction of a secure and reliable information society.

Keywords: Information Technology; Data Security; Vulnerabilities; Cryptography.

1. Introduction

Computer information technology plays a crucial role in modern society, bringing tremendous convenience to our lives and work. However, with the rapid development and widespread application of information technology, data security issues are increasingly prominent. Data security vulnerabilities have become a challenge that we must take seriously. This article aims to study the data security vulnerabilities in computer information technology and the corresponding encryption techniques in order to provide valuable guidance and insight. By gaining a deep understanding of the types and impacts of data security vulnerabilities, as well as the principles and applications of encryption technology, we can better comprehend and mitigate data security risks, thereby further safeguarding the data security of individuals and organizations.

2. Data Security Breach

2.1. Definition

Data security vulnerabilities refer to weaknesses and flaws in computer systems or networks that may enable attackers, such as hackers, viruses, trojans, or botnets, to access, tamper with, or disclose sensitive information, thereby impacting users' rights and the economic interests of businesses. In other words, data security vulnerabilities encompass various vulnerabilities or weaknesses in computer systems or networks, which when exploited by malicious actors, pose uncertain and significant threats to information security. With the widespread use of internet applications and the rapid advancement of computer technology, data security vulnerabilities continue to emerge. Sometimes, vulnerabilities may result in computer crashes or malfunctions, while other times they may lead to the loss or disclosure of personal privacy or property. Different categories of vulnerabilities may give rise to different risks and hazards, including but not limited to the following:

(1) Network attacks: Attackers exploit vulnerabilities in computer networks to gain control over computers or servers and obtain valuable information or data.

(2) Data breaches: System vulnerabilities or human negligence result in the theft, tampering, or disclosure of sensitive data or confidential files from databases to unauthorized individuals.

(3) Social engineering attacks: Intruders access users' personal information through methods such as phone solicitation and social engineering to obtain sensitive information like account passwords for unauthorized intrusions [1].

(4) Malware attacks: Malicious programs or viruses intercept information, implant advertisements, and steal sensitive information, such as user data and passwords, from computers.

Due to the potential risks and impacts of data security vulnerabilities, information security has become a pressing issue that requires serious attention. Protecting data requires the implementation of a series of strategies and technological measures.

2.2. The Impact and Risk Assessment of Data Security Vulnerabilities

The presence of data security vulnerabilities can have widespread effects and potential risks. Firstly, economic loss is an important aspect. Hacker attacks and data breaches can lead to the leakage of trade secrets, customer information, or financial data, resulting in paralyzed business operations or financial losses. Individuals may also face the risk of economic losses such as stolen property or identity theft. Secondly, user privacy leaks are serious consequences that data security vulnerabilities may bring. If hackers are able to obtain sensitive information such as personal identification, bank accounts, social media accounts and other personal data, it could be used for illegal property theft, fraudulent activities or other forms of personal harm. In addition, data security vulnerabilities may also damage the reputation of companies. Once data is leaked or customer information is disclosed, the reputation of the company may be seriously affected. Reduced user trust and loyalty could put the company at a disadvantage in the market competition. Furthermore, if data

breaches violate applicable privacy protection regulations, companies may face legal action and fines, further damaging the company's reputation and financial status. Finally, large-scale data security vulnerabilities may pose a threat to national security. For instance, hacker attacks may lead to the data and information of government agencies, military systems or critical infrastructure being stolen, destroyed, or tampered with, thereby endangering national security and economic stability. To evaluate the risk of data security vulnerabilities, a comprehensive risk analysis is needed. This includes considering the severity of the vulnerability, the types of data that may be attacked, the motivation and ability of potential attackers, the security measures and protective capabilities of the system, and other factors [2]. Based on the results of the risk assessment, corresponding security strategies and measures can be developed to mitigate potential risks and enhance the security of data. The importance of data security and corresponding prevention measures is a critical aspect of ensuring the interests of individuals, enterprises, and nations.

3. Cryptography

3.1. Definition and Explanation of Principles

Encryption technology is a mechanism that transforms plaintext data into ciphertext, ensuring its confidentiality, integrity, and availability. During the encryption process, data is converted according to specific algorithms and encryption keys, resulting in encrypted data that is difficult for unauthorized individuals or computer systems to access. Without the correct decryption key, encrypted data cannot be deciphered or understood. Only individuals or systems with the proper decryption key can decrypt the data and transform it into readable plaintext, thereby safeguarding its confidentiality and integrity. The essence of encryption technology lies in the use of unpredictable keys to encrypt plaintext, generating ciphertext. Only those in possession of the key can successfully decipher the ciphertext into plaintext. The strength of an encryption algorithm depends on the length of the key and the complexity of the algorithm. Thus, longer and more complex keys provide greater difficulty for decryption, ensuring higher security for the encryption algorithm. Encryption technology finds extensive applications in computer and network systems to safeguard sensitive data. For instance, encryption technology can protect data transmission and storage on the internet, including online banking transactions and emails. Additionally, encryption technology can be utilized to secure files or disk drives from unauthorized access, copying, or tampering. In summary, encryption technology serves as a fundamental means to protect sensitive data and ensure information security in computer and network systems. It achieves this by transforming plaintext into ciphertext and using secure keys and algorithms to process the ciphertext, guaranteeing the confidentiality, integrity, and availability of data during transmission, storage, and processing.

3.2. Classification of Encryption Techniques

Encryption techniques can be grouped into different categories based on various criteria, and the most commonly used classification is based on the usage of keys, dividing them into symmetric encryption and asymmetric encryption.

(1) Symmetric Encryption:

Symmetric encryption refers to a method where the same key is used for both encryption and decryption. In symmetric encryption algorithms, the encryption and decryption processes utilize the same key, also known as a single-key encryption. The advantage of symmetric encryption algorithms lies in their fast encryption and decryption speeds, making them suitable for encrypting and decrypting large amounts of data. Common symmetric encryption algorithms include DES (Data Encryption Standard), 3DES (Triple DES), and AES (Advanced Encryption Standard). DES is a relatively older but classic encryption algorithm that uses a 56-bit key for data encryption. 3DES is an improved version based on DES, using a 168-bit key. AES, on the other hand, is an efficient and secure encryption algorithm with key lengths of 128, 192, or 256 bits [3].

(2) Asymmetric Encryption:

Asymmetric encryption refers to a method where different keys are used for encryption and decryption. In asymmetric encryption algorithms, there is a pair of keys known as the public key and private key. The public key is used for encrypting data, while the private key is used for decrypting data. Asymmetric encryption algorithms are commonly used in scenarios such as key exchange, digital signatures, and authentication. Common asymmetric encryption algorithms include RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography). RSA is an encryption algorithm based on large number factorization, with public key lengths typically being 1024, 2048, or 4096 bits, while the key length can be set to any desired length. ECC, on the other hand, is an encryption algorithm based on elliptic curve discrete logarithm, achieving the same level of security with smaller key sizes. Key lengths for ECC usually range from 128 to 256 bits.

In addition to symmetric and asymmetric encryption, there are other classifications of encryption techniques:

(1) Stream ciphers: Stream ciphers are encryption algorithms that generate ciphertext by combining a generated stream with plaintext through mathematical operations. In stream ciphers, the bit streams of plaintext data and the key are mixed using a specific algorithm to produce the ciphertext. Common stream ciphers include RC4 and ChaCha20.

(2) Block ciphers: Block ciphers divide the plaintext into fixed-size blocks of data and encrypt these blocks using a fixed-length key. Block ciphers process one data block at a time, moving on to the next block until all blocks have been encrypted. Common block ciphers include AES and Blowfish.

These classifications help us understand different types of encryption techniques and their applications. By integrating symmetric and asymmetric encryption, along with other types of encryption techniques, we can provide enhanced security measures to meet various security requirements.

3.3. Common Encryption Algorithms and Protocols

In the realm of computer and network security, there exist numerous prevalent encryption algorithms and protocols that are widely employed to ensure the security and privacy of data. Presented below are several common encryption algorithms and protocols:

(1) SSL/TLS

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are protocols used to safeguard the security of network communication. Through the amalgamation of symmetric and asymmetric encryption, SSL/TLS ensures the confidentiality and integrity of data transmission between

communicating parties. SSL/TLS is extensively utilized in websites, e-commerce, and cloud services, with the HTTPS protocol being constructed upon SSL/TLS for secure communication.

(2) RSA

RSA is an asymmetric encryption algorithm extensively applied in fields such as digital signatures, key exchange, and authentication. The security of RSA is based on the difficulty of prime factorization, with public key lengths typically being 1024, 2048, or 4096 bits. RSA finds application in major security protocols and systems, such as SSL/TLS, SSH (Secure Shell), and PGP (Pretty Good Privacy).

(3) AES

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm that is widely recognized as the most secure and commonly used encryption standard to date. It employs 128, 192, or 256-bit keys for encrypting and decrypting data. AES finds applications in various areas such as file encryption, database encryption, and network communication encryption. The security of AES stems from its robust encryption strength. By utilizing longer key lengths and complex encryption algorithms, deciphering the ciphertext becomes exceedingly challenging. Even with brute force attacks, it requires a substantial amount of time and immense computational resources. AES supports multiple key lengths, allowing users to choose different security levels as per their requirements [4]. Furthermore, AES exhibits exceptional performance capabilities. Its encryption and decryption processes have been meticulously designed to execute efficiently on various computing devices, be it in hardware or software form. Consequently, AES has become a widely adopted encryption algorithm, offering protection not only for sensitive data on personal computers but also for critical information on enterprise servers, as well as securing data in cloud computing and Internet of Things (IoT) devices. To sum up, AES is a highly secure and efficient encryption algorithm that has found broad application in diverse fields. It plays a vital role in safeguarding the confidentiality of data, providing reliable security measures to individuals and organizations alike. Whether for personal or enterprise use, employing the AES encryption algorithm ensures the confidentiality and integrity of sensitive information, effectively preventing data leaks and unauthorized access.

(4) DES

The Data Encryption Standard (DES) is a symmetric encryption algorithm that was initially released and adopted by the National Institute of Standards and Technology (NIST) in 1977. DES uses a 56-bit key to encrypt and decrypt data, and divides plaintext into 64-bit blocks which are transformed through a series of complex mathematical operations. For many decades, DES has been widely used as a standard encryption protocol, playing a crucial role in financial transactions and governmental departments. However, as computing power continues to evolve, the security of DES has become increasingly questionable. Due to the short key length of DES, it is vulnerable to attacks such as brute force cracking. To enhance the security of encryption, modern algorithms such as Advanced Encryption Standard (AES) have replaced DES. Compared with DES, AES features longer key lengths (128-bit, 192-bit, or 256-bit), more complex encryption algorithms, and is considered a more secure and reliable encryption standard. Despite the security issues with DES, it is still used in certain specific scenarios. For example, some legacy financial systems and hardware modules may still use DES encryption. However, to better protect data security, it is highly recommended to use more powerful and secure encryption standards such as AES to replace DES.

(5) Blowfish

Blowfish is a symmetric encryption algorithm that permits the use of variable-length keys, ranging from 32 to 448 bits. Blowfish finds widespread application in various software and hardware systems, including virtual private networks (VPNs), encrypted file systems, and wireless communication networks.

In addition to the aforementioned encryption algorithms and protocols, there exist many other common encryption algorithms and protocols, such as ECC (Elliptic Curve Cryptography), SHA (Secure Hash Algorithm) series, DSA (Digital Signature Algorithm), and PGP (Pretty Good Privacy). These encryption algorithms and protocols play crucial roles in different domains and applications, safeguarding the privacy and security of data. When choosing and implementing encryption algorithms and protocols, one must carefully consider and select based on specific requirements and security needs to ensure the secure transmission and storage of data.

3.4. Application of Encryption in Data Security

The wide and significant application of encryption technology in data security cannot be overemphasized. It is mainly applied in data transmission security, data storage security, and identity authentication. In data transmission, encryption technology guarantees that data is not intercepted, tampered with, or falsified while being transmitted from the sender to the receiver. Symmetric or asymmetric encryption algorithms can be used to protect sensitive information such as personal privacy, payment data, and corporate secrets during network transmission. Common applications include HTTPS protocol encrypted with SSL/TLS and VPN communication encryption. Data storage security is also an important application field of encryption technology. By encrypting data stored in computers, servers, or cloud services, data confidentiality can be maintained even in cases of theft or unauthorized access. This encryption method can be applied to various scenarios such as personal computers, mobile devices, databases, and cloud storage. Common applications include full-disk encryption, file encryption, database encryption, and transparent data encryption. Identity authentication is another critical field that requires encryption technology. By using encryption technology, the security of user identity and authentication information can be ensured during transmission and storage. Digital certificate and digital signature schemes that use asymmetric encryption algorithm are used to verify and confirm the identities of both parties in communication, to prevent impersonation and forgery. This technology is widely used in website authentication, email signature, and digital transactions. Apart from the aforementioned applications, encryption technology plays a role in many other fields, such as password management, Internet of Things security, healthcare, finance, and military. With the continuous development of the Internet and data exchange, the importance of data security is increasingly prominent, and encryption technology is constantly evolving and innovating to cope with the changing security threats and demands [5].

4. Conclusion

The rapid development of computer information

technology has brought great convenience and opportunities, but it has also given rise to various data security vulnerabilities and threats. Issues such as data breaches, network attacks, and identity theft have become significant challenges faced by modern society. In order to address these challenges, the research and application of encryption technology have become particularly important. The study and application of encryption technology play a crucial role in protecting the confidentiality, integrity, and reliability of data. Whether during data transmission or storage, the use of encryption technology ensures the security of data, preventing unauthorized access, theft, or tampering. Furthermore, encryption technology also facilitates identity authentication and data security verification, ensuring the legitimacy of communication parties and the accuracy of data. With the continuous development of technology, encryption techniques are constantly evolving and innovating. New encryption algorithms and protocols emerge, providing stronger protection for data security. From traditional symmetric encryption to asymmetric encryption, and then to more advanced elliptic curve encryption and quantum encryption technologies, encryption methods continue to enhance security and efficiency. Additionally, encryption research also needs to address cryptanalysis for the purpose of cracking and attacking, as well as the potential post-quantum computing era. In the field of computer information technology, the research on data security and encryption technology is an important and complex subject. It requires collaboration among various entities, including government, academia, and enterprises, involving experts and researchers from different fields. Only through continuous research, innovation, and application can we protect our valuable data in the information age and ensure a more secure and trustworthy digital life.

References

[1] Kimberly P ,T R G ,Joelle S L , et al.The centralization and rapid deployment of police agency information technologies: An appraisal of real-time crime centers in the U.S.[J].The Police Journal,2023,96(4):10-12.

[2] D.X. H T ,Van P N ,T.M. T N , et al.Information technology capabilities and organizational ambidexterity facilitating organizational resilience and firm performance of SMEs [J]. Asia Pacific Management Review,2023,28(4):33.

[3] Liza R G ,H.Y. D L ,E. B C , et al.Can we improve healthcare with centralized management systems, supported by information technology, predictive analytics, and real-time data?: A review[J].Medicine,2023,102(45):10.

[4] Sakinah P A ,Wail A A A ,Farida R , et al.Mobile Application Design for Protecting the Data in CloudUsing Enhanced Technique of Encryption[J].International Journal of Engineering Technology,2018,7(4.15):5-8.

[5] Ruizhong D ,Yuchi T ,Mingyue L .Refined statistical attacks against searchable symmetric encryption using non-indexed documents[J].Journal of Information Security and Applications, 2023,79.