Analysis of the Application of Data Encryption Technology in Computer Network Security

Xinyang Jia
Institute of Problem Solving, Xi'an FanYi University, Xi'an, Shaanxi, China

Abstract: The application of data encryption technology in computer network security has become an important means to protect sensitive information and ensure secure data transmission. This paper first provides an overview of data encryption technology, including basic concepts, classification of encryption algorithms, and encryption principles. A comparison between symmetric and asymmetric encryption algorithms is also presented. The paper then explores the application of data encryption technology in network transmission, network storage, and network communication. In addition, the basic concepts of digital signature technology are introduced, along with its implementation modes and application scenarios in network security. Furthermore, the paper discusses the basic concepts of security protocols and provides detailed explanations of the TLS/SSL security protocol and IPsec protocol. The development trends of data encryption technology are also analyzed, including the combination of multiple technologies, big data encryption, quantum encryption technology, and verification encryption. In conclusion, the application of data encryption technology in computer network security is diverse and will continue to play an important role in future developments.

Keywords: Data Encryption Technology; Computer Network Security; Network Transmission; Network Storage; Network Communication; Digital Signature Technology; Security Protocols

1. Overview of Data Encryption Technology

1.1 Basic Concepts of Data Encryption Technology

The basic concepts of data encryption technology include plaintext, ciphertext, encryption algorithm, decryption algorithm and key, etc. Clear text refers to unencrypted raw data, and ciphertext refers to data that is not easy to crack when processed by an encryption algorithm. Encryption algorithm refers to the algorithm of converting plaintext into ciphertext, and decryption algorithm refers to the algorithm of restoring ciphertext to plaintext. Key is a special parameter used in encryption and decryption, which is the key to ensure the security of the encryption and decryption process.

1.2 Encryption Algorithm Classification and Encryption Principle

The encryption algorithm is generally divided into symmetric encryption algorithm and asymmetric encryption algorithm. Symmetric encryption algorithm refers to the encryption algorithm using the same key for encryption and decryption. Its encryption speed is fast and the encryption strength is high, but the management and distribution of the key has become its main bottleneck. Common symmetric encryption algorithms are DES, 3 DES, AES and so on. Asymmetric encryption algorithm refers to the encryption algorithm that uses different keys. Its advantage is that it solves the problem of key management and distribution, and can realize the functions such as digital signature and authentication, but the encryption speed is slow and the encryption intensity is relatively low[1]. Common asymmetric encryption algorithms include RSA, ECC and so on.

1.3 Comparison of Symmetric Encryption Algorithm and Asymmetric Encryption Algorithm

Symmetrical encryption algorithm and asymmetric encryption algorithm have different advantages and disadvantages, which need to be selected according to specific situations in practical application. The advantage of symmetric encryption algorithm

lies in the fast encryption speed and high encryption intensity, but the disadvantage lies in the difficulty of key management and distribution, and the security is threatened by key leakage. The advantage of asymmetric encryption algorithm is that it can solve the problems of key management and distribution, and has the functions of digital signature and authentication, but the encryption speed is slow and the encryption intensity is relatively low.

2. Application of Data Encryption Technology in Computer Network Security

2.1. Application of Data Encryption Technology in Network Transmission

Encryption technology encrypts the raw data to generate a section of dense text. Iphertext can only decrypt and restore to raw data by obtaining the decryption key. In the network transmission, the encryption technology usually uses the transmission layer security protocol (TLS) or the secure socket layer protocol (SSL) to protect the security of the data. Both protocols use encryption to encrypt and decrypt data.

TLS protocol is a security protocol based on transmission layer, which uses various encryption technologies such as public key encryption, symmetric key encryption and message summary. When transferring data, the TLS protocol adds a piece of security header information to the packet and encrypts the data before transferring it. After receiving the data, the receiver will first decrypt the security header information, obtain the decryption key, and then decrypt the data, so as to restore to the original data.

The SSL protocol, similar to the TLS protocol, is also a security protocol based on the transmission layer. It adopts encryption technologies such as public key encryption and symmetric key encryption. When transferring data, the SSL protocol adds a piece of SSL header information to the packet and encrypts the data before transferring it. After receiving the data, the receiver will first decrypt the SSL header information, obtain the decryption key, and then decrypt the data, so as to restore to the original data.

2.2. Application of Data Encryption Technology in Network Storage

In network storage, encryption technology usually uses disk encryption or file encryption to protect the data security.

Disk encryption means that it encrypts the entire storage device, encrypting all the data on the storage device. When using disk encryption technology, you need to set an encryption password first. After the setting is complete, all of the data is automatically encrypted. When using a storage device, you need to enter the correct password to decrypt the data and read and write.

File encryption is the encryption of certain or specific files to secure them. In file encryption, you need to select the file that needs to be encrypted, and then set an encrypted password. An encrypted file can read or write only with the correct password entered.

2.3. Application of Data Encryption Technology in Network Communication

In network communication, encryption technology usually uses email encryption, instant messaging encryption and voice encryption technology to protect the security of communication data.

E-mail encryption refers to the encryption of the message content, and only the recipient can decrypt and read the message content with the corresponding decryption key. In e-mail, encryption technology usually uses encrypted accessories to achieve encryption.

Instant communication encryption refers to the encryption of instant communication content, and only the receiver can decrypt and read the content by using the corresponding decryption key. In instant communication, encryption technology usually adopts end-to-end encryption.

Voice encryption refers to the encryption of voice communication, to ensure the security of voice communication content. In voice communication, encryption technology usually uses digital voice encryption technology to achieve encryption, ensuring that the communication content is not stolen or tampered with.

3. Application of Digital Signature Technology

3.1. Basic Concepts of Digital Signature Technology

With the rapid development of computer

technology, computer network is more and more widely used in social life, including various network transactions, e-commerce and so on. Because the information transmission on the network has the risk of easy eavesdropping and tampering, so the digital signature technology comes into being[2].

Digital signature refers to a technical means used to ensure the integrity, authenticity and nondeniability of the information. Digital signature adopts asymmetric encryption technology to encrypt the information, and attach the digital signature of the signer to ensure the integrity, authenticity and nondeniability of the information, so as to realize the purpose of safe transmission and storage of information.

Digital signature technology usually adopts the principle of public key cryptography, which mainly includes two processes: signature and verification. In the signature process, the signer uses his private key to encrypt the information to produce the digital signature; In the verification process, the receiver uses the public key of the digital signature to verify the authenticity and integrity of the information.

3.2. Implementation Mode of Digital Signature Technology

Digital signature techniques usually employ asymmetric encryption techniques, including encryption algorithms such as RSA and DSA. The RSA algorithm is currently recognized as one of the most secure asymmetric encryption algorithms, and its basic principle is to use the product of two large prime numbers as the public key, with one large prime number as the private key. DSA algorithm is based on the discrete logarithmic problem, including three processes of key generation, signature and verification.

Digital signature technology mainly includes the following steps:

(1) Key generation. The signer generates his own public key and private key, and the public key public, the private key confidential.

(2) Signature. The signer uses his own private key to encrypt the information to generate a digital signature.

(3) Validation. The receiver uses the public key to decrypt the digital signature to verify the authenticity and integrity of the information.

3.3. Application Scenarios of Digital Signature Technology in Network Security

Digital signature technology has a wide range of applications in network security, including the following aspects:

(1) E-commerce. In e-commerce, digital signature technology can be used to guarantee the authenticity and integrity of transactions and prevent information from being tampered with or fake.

For example, when shopping in an online store, users can use the digital signature technology to sign the order information to ensure the authenticity and integrity of the order information.

(2) Email. In e-mail, digital signature technology can be used to verify the sender and prevent messages from being tampered with. For example, users can use digital signature technology to sign sent messages to ensure that the content is not tampered with and to prevent messages from being fake.

(3) Digital copyright protection. Digital signature technology can be used to protect digital rights and prevent piracy and unauthorized reproduction. For example, in the transmission and storage of digital music and digital video, digital signature technology can be used to digital sign music files and video files to ensure the security and protection of copyright.

(4) Authentication. Digital signature technology can be used for authentication to prevent identity fraud and fraud. For example, when logging in to a website, users can use digital signature technology to verify their identity to ensure the security of the login account.

(5) Data backup. Digital signature technology can be used for data backup to ensure the integrity and authenticity of the backup data. For example, enterprises and organizations can use digital signature technology to sign the backup files to ensure that the backup files are secure and correct.

4. Application of the Security Protocol

4.1. Basic Concept of Security Agreement

Security protocol refers to the protocol used to guarantee communication security in computer network communication. The function of the security protocol is to provide a secure data transmission and client authentication in an

insecure communication environment. Security protocol adopts encryption technology and authentication technology to ensure the integrity, confidentiality and credibility of communication data and prevent illegal users from stealing or tampering with communication data.

Security agreements usually include the following:

(1) Authentication: The purpose is to confirm the identity of both parties to ensure the security and credibility of the communication.

(2) Encryption technology: encryption technology is used to encrypt the data to ensure that the communication data is not illegally obtained and stolen.

(3) Digital signature: digital signature technology is adopted to ensure the integrity and certification of the data.

(4) Access control: control and authorize sensitive resources through access control technology.

(5) Security management: security management technology is used to manage and monitor network resources to ensure network security.

4.2.TLS/SSL Detailed Explanation of the Security Protocol

The TLS / SSL protocol is an encryption protocol widely used in the Internet to ensure secure the transmission of web pages and applications. TLS / SSL protocol adopts public key encryption technology to confirm the identity of both parties through the digital certificate trust chain mechanism to ensure the integrity, confidentiality and credibility of the communication data.

The TLS / SSL protocol mainly includes the following parts:

(1) Handshake agreement: it is used to establish a secure channel and confirm the identity of both parties, and complete the identity authentication through the RSA digital certificate authentication mechanism.

(2) Encryption protocol: the symmetric key encryption algorithm is used to encrypt the data to ensure the confidentiality of the communication data.

(3) Identity authentication protocol: the digital certificate mechanism is adopted to authenticate the identities of both communication parties, and the credibility of the communication data is ensured through the digital certificate trust chain mechanism.

(4) Alert protocol: it is used to send alarm information, such as identity authentication failure, key expiration, etc., to ensure communication security.

4.3. IPsec Detailed Explanation of the Protocol

IPsec protocol is a protocol used to guarantee the safe transmission of IP packets. The encryption technology includes symmetric key encryption, asymmetric key encryption, etc. The IPsec protocol can be divided into two modes: transmission mode and tunnel mode[3].

(1) Transmission mode: it is suitable for the communication between the two hosts to ensure the confidentiality of the communication data, but it does not involve the integrity and authentication of the data.

(2) Tunnel mode: suitable for the communication between the host machine and the gateway, to ensure the confidentiality, integrity and authentication of the communication data.

The main features of the IPsec protocol include:

(1) Data encryption: symmetrical key encryption technology is used to encrypt data to ensure the confidentiality of communication data.

(2) Data integrity: Use encryption hash algorithm and digital signature technology to ensure the integrity of communication data.

(3) Data authentication: the digital certificate mechanism is adopted to authenticate the identity of both parties to ensure the credibility of the communication data.

4.4. Application Scenarios of Security Protocol in Network Security

Security protocol is an important means to ensure network security, and it is widely used in the following scenarios:

(1) Safe transmission website: the security protocol is mainly used to ensure the safe access of the website, to ensure the security of users' login information and transmission data.

(2) E-commerce: The security agreement is mainly used to ensure the secure data transmission and payment process of e-commerce, and to ensure the security of users' shopping and payment information.

(3) Enterprise VPN: The security agreement is mainly used to ensure the security of the

enterprise's internal communication and ensure that the enterprise confidential information is not illegally stolen or tampered with.

(4) Mobile communication: The security protocol is mainly used to ensure the secure data transmission and identity authentication of mobile communication, and to ensure the security of users' mobile communication information.

5. The Development Trend of Data Encryption Technology

5.1. Development Process of Data Encryption Technology

The development of data encryption technology can be traced back to the ancient cryptography, when people simply used simple replacement, displacement and other technologies to encrypt messages. With the development of computers, data encryption technology has been widely used. From the initial symmetric encryption algorithm, to the later asymmetric encryption algorithm, and then to the current quantum key distribution and other technologies, the development process of data encryption technology is long and interesting.

5.1.1. Symmetric encryption algorithm

Symmetric encryption algorithm is one of the earliest data encryption technologies. It uses the same key to add and decrypt messages. The confidentiality of the key is very important. The earliest symmetric encryption algorithms mainly include Caesar password, replacement password, DES algorithm and so on.

Among them, the Caesar password is one of the oldest encryption techniques, which uses a fixed offset to encrypt messages. Permutation password is to replace each character in the plaintext according to the predetermined rules after getting the ciphertext.

DES algorithm is one of the classical algorithms in symmetric encryption algorithm. It uses a 56-bit key to encrypt the plaintext according to the prescribed rules. The plaintext is 64 bits each time, and the cryptotext is also 64 bits. However, with the improvement of computer computing power, the security of DES algorithm was threatened, so the more secure AES algorithm was later developed.

5.1.2. Asymmetric encryption algorithm

An asymmetric encryption algorithm is an algorithm, one of which is disclosed, called a public key, and the other is a secret, called a private key. The most well-known asymmetric encryption algorithm is the RSA algorithm.

The RSA algorithm is an encryption technology based on the large number factorization. It uses the public key to encrypt the plaintext during the data transmission process, and the ciphertext can only be decrypted by using the private key. RSA algorithm has its long key length, high security, and can be applied to digital signatures.

5.1.3. Quantum key distribution

Quantum key distribution is an encryption technology based on the principle of quantum entanglement. In the process of data transmission, the quantum state is used to transmit the key, and the security of the key is guaranteed by the special properties of the quantum state.

Quantum key distribution technology requires the use of special devices, such as quantum key distributors, that can produce and control quantum states. Although the quantum key distribution technology is still in the experimental stage, it is considered to be one of the effective means to ensure information security in the future[4].

5.2. Future Development Trend of Data Encryption Technology

Data encryption technology plays an important role in computer network security, It can ensure the data security in the process of network transmission and protect personal privacy information. The future development trend of data encryption technology is mainly reflected in the following aspects:

5.2.1. Combination of multiple technologies

Future data encryption technologies will no longer use only one encryption technology, but will combine multiple technologies to improve the security of the encryption algorithms. For example, the combination of symmetric and asymmetric encryption algorithms can improve the strength and efficiency of the encryption algorithms.

5.2.2. Big Data Encryption

In the era of big data, protecting the security of big data has become an important issue. In the future, data encryption technology needs to combine machine learning, deep learning and other technologies to encrypt and decrypt large amounts of data to ensure the security and privacy of data.

5.2.3. Quantum encryption technology

With the development of quantum computing technology, the future data encryption technology needs to combine quantum computing technology, and use quantum key distribution and other technologies to ensure the security of data. Quantum encryption technology has the unpredictability and confidentiality of quantum states, which is an important development direction of future data encryption technology.

5.2.4 Verify the encryption

Future data encryption technology needs to be verifiable enough to verify the encryption and decryption process to ensure the integrity, reliability and authenticity of the data during the transmission process. Therefore, verifiable encryption technology will be one of the development trends of future data encryption technology.

6. Conclusions

This paper to the application of data encryption technology in computer network security as the research object, through the principle of encryption technology, classification, application and development trend systematically summarized and analysis, put forward the widely used in the computer network encryption algorithm and protocol, explore the encryption technology in the field of network security application and development direction, with the following innovation:

(1) Comprehensively summarize the classification, working principle, application and development trend of data encryption technology, and conduct in-depth analysis and evaluation of different types of encryption algorithms and protocols, providing useful reference and guidance for readers.

(2) Through the analysis of the encryption protocol SSL / TLS, the existing shortcomings are found, and the solutions are proposed.

References

[1] Ahmadi S. Challenges and Solutions in Network Security for Serverless Computing[J]. International Journal of Current Science Research and Review, 2024, 7(1): 218-229.

[2] Liu J. Research on Computer Network Secure Communication and Encryption Algorithm Based on Machine Learning[C]//2023 Asia-Europe Conference on Electronics, Data Processing and Informatics (ACEDPI). IEEE, 2023: 113-117.

[3] Peng Y. Research on the Technology of Computer Network Security Protection[J]. Journal of Applied Data Sciences, 2023, 4(1): 22-29.

[4] Adeniyi A E, Abiodun K M, Awotunde J B, et al. Implementation of a block cipher algorithm for medical information security on cloud environment: using modified advanced encryption standard approach[J]. Multimedia Tools and Applications, 2023: 1-15.

