Computer Network Communication Security Data Encryption Technology Postprint

Authors: Bai Rongjian

Date: 2023-10-08T00:00:00+00:00

Abstract

In the contemporary era of rapid network information development, network communication has permeated numerous social sectors, playing a significant role in driving societal advancement and enhancing the convenience of people's daily lives. However, the characteristics of computer networks—including interconnectivity, openness, and uneven distribution—combined with deficiencies in other technologies, have led to frequent network communication security incidents that severely impact user experience. As confidentiality requirements for online activities continue to escalate, the application of data encryption technology safeguards the confidentiality demands for personal data and related information in network activities, thereby ensuring network security and confidentiality.

Full Text

Preamble

Research · Application and Engineering: Computer Network Communication Security Data Encryption Technology

Abstract: In today's era of rapid network information development, network communication has permeated numerous social domains, playing a crucial role in driving social progress and facilitating people's daily lives. However, computer networks exhibit characteristics such as interconnectivity, openness, and non-uniform distribution, coupled with technological deficiencies, leading to frequent network communication security incidents that seriously impact users. Consequently, confidentiality requirements for online activities are increasingly stringent. The application of data encryption technology ensures that individuals can maintain confidentiality of their data and related materials during network activities, thereby guaranteeing network security and privacy.

Keywords: network communication; data encryption
Classification: TJ768
Document Code: A
Article ID: 1671-0134(2017)12-106-02
DOI: 10.19483/j.cnki.11-4653/n.2017.02.030
Author: Bai Rongjian, Program-controlled Telephone Department, Technical Bureau, Xinhua News Agency

1. Computer Network Communication and the Necessity of Data Encryption

The fundamental approach is to disguise information to prevent leakage during storage and transmission. In most cases, data encryption technology is divided into symmetric encryption and asymmetric encryption techniques.

1.1 Computer Network Communication

Network communication refers to the effective connection of independent hosts and workstations through physical links, forming data links between multiple networks to achieve communication and resource sharing. Network communication primarily involves network protocols, which establish connections for information exchange and sessions. These protocols specify standards for controlling code transmission, information transfer speeds, and transmission procedures.

1.2 Necessity of Data Encryption

Data encryption technology constitutes the core of data security techniques. Particularly in today's internet era, where everyone uses the internet daily, important information such as financial data and documents faces potential threats. This has drawn significant attention to protecting data from theft, tampering, and destruction. Data encryption technology is the key to addressing these issues. Statistics show that 20% of security threats stem from unauthorized internal access, while internal security threats exceed 80%. Electronic document leaks account for over 30% of damages caused by security vulnerabilities. Common intranet security measures such as firewalls cannot effectively prevent the leakage of corporate confidential information. Therefore, data encryption is crucial for defending against both external and internal threats.

2. Key Cryptography Technology

The origins of cryptography can be traced back to ancient Egyptian hieroglyphs. Cryptography studies how to ensure the security of confidential information through encoding techniques, comprising two branches: cryptology and cryptanalysis. A cryptographic system typically performs both encryption and decryption transformations. Encryption employs an encoding algorithm to convert

original information into an incomprehensible code, thereby protecting confidential information. Decryption is the inverse process, using a decryption algorithm to restore the incomprehensible information to its original form, though decryption is considerably more difficult than encryption. Cryptographic technology encompasses cryptography design, cryptanalysis, and key management, with the primary goal of cryptography design being to ensure information confidentiality.

3. Two Common Data Encryption Technologies

3.1 Symmetric Data Encryption

Symmetric encryption is the fastest and simplest encryption method, using the same key for both encryption and decryption. Key size must balance security and efficiency. Symmetric data encryption technology features public algorithms, fast encryption speeds, minimal computational overhead, and high encryption efficiency. Symmetric encryption typically uses relatively small keys, generally less than 256 bits. While larger keys provide stronger encryption, they also slow down the encryption and decryption processes. For instance, a 2-bit key would allow hackers to easily attempt decryption using 0, 1, and 2. Conversely, a 1 MB or larger key might be theoretically unbreakable but would require extremely long encryption and decryption times.

3.2 Asymmetric Data Encryption

Asymmetric encryption provides a highly secure method for data encryption and decryption, utilizing a pair of keys: a public key and a private key. Asymmetric encryption uses one of these keys for encryption, while decryption requires the other. The private key must be securely maintained by one party and never disclosed, whereas the public key can be distributed to anyone who needs it. The process of confidential information exchange using asymmetric encryption algorithms proceeds as follows: Party A generates a key pair and publicly releases one key as the public key; Party B obtains this public key, uses it to encrypt information, and then transmits the encrypted data to Party A; Party A then decrypts the confidential information using their exclusive private key. Party A can only decrypt information that has been encrypted with their corresponding public key.

4. Encryption Implementation Methods

4.1 Link Encryption

Link encryption, sometimes called link-level or link-layer encryption, involves encrypting data before transmission over network communication links. Essentially, every node machine throughout the network performs encryption and decryption, and each node must be equipped with cryptographic devices capable of both operations. During the entire transmission process, data must be decrypted and then re-encrypted at each link or node. Throughout transmis-

sion, data appears in ciphertext form. To ensure communication security, the data does not reveal information about the sending or receiving points, nor does it display information frequency or length. The data link layer corresponds to the second layer in the OSI architecture, with each link utilizing a different key. This ensures that if a key on one link is compromised, encrypted information on other links remains secure.

4.2 End-to-End Encryption

End-to-end encryption does not require intermediate nodes to perform encryption or decryption; information is encrypted at transmission and decrypted upon receipt. For convenience, encryption can also be implemented via software. Under end-to-end encryption, a virtual confidential channel exists between users. The total number of keys equals the number of user pairs, with keys shared between each pair. From an identity authentication perspective, link encryption can only authenticate nodes. For example, using node A's key for a message only guarantees that it originated from node A, but it could still be another user passing through node A. End-to-end encryption is visible to users, making the source and sender of files clearly identifiable. For pairwise communication among multiple users, a total of n×(n-1)/2 keys are required, with each user needing (n-1) keys. As the number of online communication users increases, so does the number of keys. For security purposes, keys must be replaced periodically, with some keys used only once in special circumstances, which creates substantial key management overhead.

5. Application of Data Encryption Technology in Computer Network Communication

Currently, e-commerce is thriving, significantly promoting social progress and providing considerable convenience for people's work and daily lives. The internet was originally designed merely to provide users with a flexible, fast communication platform. To ensure the sustained, rapid, and healthy development of e-commerce, electronic transactions involved in e-commerce must be conducted over the internet, which lacks the security of commercial transactions. Therefore, a secure computer network environment is essential, primarily manifested in the security of transaction information within the network. Data security encryption technologies such as SET security protocols, SSL, digital signatures, and certificates can be applied in e-commerce activities to effectively prevent information data leakage and breaches between transacting parties.

5.2 Data Encryption Technology in Computer Software

With the continuous development of computer network communication, computer software has also experienced rapid advancement. If antivirus software becomes infected with a virus during the data encryption process, it becomes impossible to verify whether programs or data have valid signatures. Therefore,

when encrypting programs, files slated for encryption or decryption should be scanned for viruses. Many hackers exploit virus-infected software to steal information during data exchange, severely impacting users. Consequently, encrypting software is crucial. Using data encryption technology to encrypt application software can ensure that user data is not stolen, while early warning systems can report and provide feedback on network security issues for user remediation. Users should regularly inspect application software to ensure security, promptly and effectively addressing deeply embedded viruses to maintain data information security.

5.3 Data Encryption Technology in LANs

Nowadays, many industries have established internal local area networks (LANs) to improve work efficiency and applications, placing substantial amounts of data information in network environments for rapid transmission and important notifications. Without effective protective measures, this would undoubtedly pose serious risks to companies and employees. Data encryption technology in LANs primarily involves technical encryption of data information through routers and senders. This not only ensures the security of data transmission within the LAN but also defends against external attacks, thereby protecting critical internal company information from theft and destruction.

5.4 Data Encryption Technology in Virtual Private Networks

Currently, most companies have established their own private office network systems, using LANs to share internal data. However, branch offices require cross-regional operations, necessitating leased dedicated lines to connect various branch LANs into a wide area network (WAN) to support data sharing. Nowadays, routers with encryption and decryption capabilities are available. When the sender's data information leaves the VPN, the router encrypts it; during transmission, it remains in ciphertext form. Upon reaching the destination LAN, the router decrypts the ciphertext, allowing the receiving user to view the sender's data information. This approach ensures data security while maintaining simple and convenient transmission methods.

6. Conclusion

Computer communication network security requires our full attention as it represents an objective reality. We should further strengthen communication security protections. Currently, computer network security is receiving increasing attention as information security becomes a major concern. Hackers continuously emerge in the network security landscape, causing personal information leaks. With the widespread application of computer network communication technology bringing significant convenience to people's production and daily lives, the importance of computer network communication security data encryption technology in network security becomes evident.