The Application of Data Encryption Technology

Yuanbiao Zhou

09/9/2022

George Mason University IT 104-003

George Mason University Honor of Conduct

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://oai.gmu.edu/mason-honor-code/ and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material1 copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site."

The application of Data Encryption Technology

Introduction

With the development of network technology, the network is providing people with great convenience. But due to the openness of the Internet itself, there are many hidden dangers in the network, like viruses, hacker attacks and computer threats have become commonplace, and make information disclosure. “What prevents nefarious actors from stealing information and money every time someone engages in a personal transaction online? The answer is encryption. Cryptography is the process of scrambling messages so that only desired parties can unscramble and discern their meanings by using secret keys. (Harmon, P. 2022)” Therefore, the confidentiality of information is an important aspect of information security. The purpose of confidentiality is to prevent unauthorized users from cracking confidential information. Encryption is an important means to achieve information confidentiality.

Current Use

In recent years, with the rapid development of the e-commerce industry, more and more people have formed the habit of shopping on the Internet, and the most important thing to protect is the property and privacy security of users. In order to protect the legitimate rights and interests of users, almost all e-commerce platforms will choose to use the corresponding encryption technology to improve the security of websites. Encryption technology is the main security and confidentiality measure adopted by e-commerce and is the most commonly used security and confidentiality means. It uses technical means to transform important data into garbled code (encryption) for transmission and then uses the same or different means to restore (decrypt) after

arriving at the destination. The application of encryption technology is multifaceted, but the most extensive application is in e-commerce and VPN, which is loved by the majority of users. “Intel and a slew of other hardware manufacturers are behind a wave of new devices designed to make encryption faster and more secure. These products are the latest evidence that encryption, essential for secure electronic commerce and communications via the Internet, is migrating from software-based technology to hardware-and the pace is picking up (Joachim, D. 1997)”.

E-business requires that customers can do many kinds of business activities on the Internet without worrying about their information being stolen. In the past, in order to prevent the number of the information from being stolen, users usually register some accounts with their information or ordered by phone and paid with their credit card. People began to use RSA (a public/private key) encryption technology to improve the security of information transactions, therefore, making it possible for e-business to become virtual.

Security Aspects

In order to solve the data security problem of key businesses, it is essential to first make a comprehensive, reliable, secure and multi-level backup of the data system. In addition, all kinds of security products, no matter firewall, anti-virus, anti-hacker, anti-intrusion, are more or less responsible for protecting data. From the perspective of data protection, the broad concept of data security can be divided into three parts: data encryption, data transmission security and identity authentication management. Data encryption is to transform sensitive plaintext data into unrecognized ciphertext data according to the determined cryptographic algorithm. By using different keys, the same plaintext can be encrypted into different ciphertext using the same encryption algorithm. When necessary, you can use the key to restore the ciphertext data to plaintext data, which is called decryption. In this way, data confidentiality can be achieved. Data

The application of Data Encryption Technology

encryption is recognized as the only practical method to protect the security of data transmission and an effective method to protect the security of stored data. It is the most important line of defense for data protection in technology.

"Professional hackers are using more sophisticated techniques to try to steal valuable corporate data. One strategy involves making unwitting accomplices among employees-or employees of business partners-who allow intrusions into systems" (Sivarama, Krishnan, 2011). Data encryption technology is the most basic security technology, known as the core of information security. It was originally used to ensure the confidentiality of data during storage and transmission. It replaces the protected information into ciphertext through transformation, replacement and other methods, and then stores or transmits the information. Even if the encrypted information is obtained by unauthorized personnel during storage or transmission, it can ensure that the information is not recognized by them, so as to achieve the purpose of protecting information. The confidentiality of this method depends directly on the cryptographic algorithm and key length.

Ethical and Social Implications

Law enforcement agencies believe that encryption also allows criminals to communicate securely. If ordinary criminals or terrorists encrypt their communications, it is more difficult for law enforcement personnel to disrupt their plans and identify and capture those responsible for harmful illegal acts. Recently, hackers have also deployed "ransomware," that is, software that encrypts the files of innocent victims, and then ask for payment in exchange for a decryption key.

The application of Data Encryption Technology

Some people call for the development of encryption technology to allow law enforcement investigators to decrypt information only when needed, but not for others to do the same. In response, network security experts believe that if it is not provided to hackers and other people who will cause harm, it is impossible to grant such access rights to "good people". “Do we have an absolute right to privacy for our communications? In Europe, for example, privacy is deemed to be a basic human right. Even in European countries, however, the debate about encryption is raging, because the right to privacy (which encryption protects) is balanced against other rights—such as the right to life and security. (University, S. C. 2016, December 2).”

Future Use

With the rapid development of network technology and information technology and the continuous improvement of computer computing speed, data encryption technology may not meet people's needs, and people urgently need new cryptographic systems. The future quantum cryptography, DNA cryptography, chaotic cryptography and other cryptographic technologies are being explored and studied. Quantum cryptography uses physical principles to protect information. Quantum encryption is the use of quantum to make passwords. It breaks through the constraints of traditional encryption methods, and the quantum state as the key is not replicable, which can be said to be absolutely safe.

Conclusion

Information encryption is the most basic and core technical measure and theoretical basis to ensure information security. Information encryption is also a major part of modern cryptography. Information encryption is the most basic and core technical measure and theoretical basis to ensure information security. Information encryption is also a major part of modern cryptography. To ensure better continuity of the development of computer networks, it is

necessary to develop towards the direction of network system management and security management and comprehensively improve the design. Computer network security management awareness, thereby effectively avoiding or reducing attacks by hackers and virus damage. The more advanced the network, the more important the security. In our daily work, we always regard the safe and stable operation of the system as an important task of information technology and take measures to ensure that.

References

1. Harmon, P. (2022). Data breach notification laws and the quantum decryption problem. *Washington and Lee Law Review, 79*(1), 475-519. Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/scholarly-journals/data-breach-notification-laws-quantum-decryption/docview/2681520533/se-2

This citation is helpful because it is talking about encryption technologies and some information disclosed. It can be caused losses. Also, many people start to use internet to trade, there is possible to cause their identity be theft. That may use their information to their money or something important.

2. Joachim, D. (1997). Hardcore security -- chip-level implementation bolsters encryption technology for electronic commerce. *Communications Week,* (646), 1. Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/trade-journals/hardcore-security-chip-level-implementation/docview/226888362/se-2

This citation is helpful because it is talking about a lot of risks and encryption technology in the field of electronic commerce. Also, encryption technology may be directly embedded into hardware and chips or core of PCs.

3. Santa Clara University. (2018). Ethical Questions About Encryption. Retrieved September 13, 2022, from @SantaClaraUniv website: https://www.scu.edu/ethics/focus-areas/technology-ethics/resources/ethical-questions-about-encryption/

This citation is helpful because it is talking about some ethical questions about encryption in many aspects. One hand is that some people think that encryption also allow criminals to communicate securely. On the other hand, encryption can protect people's information and prevent hackers from internet. Some people think encryption can do more good than harm.

4. Managing information security risks: Sivarama krishnan writes about how organizations can go about handling risk in the era of cloud computing.(2011). *Express Computer,* Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/trade-journals/managing-information-security-risks/docview/873627573/se-2

This citation is helpful because it is talking about some security risks, understanding the security risks and how to prevent. Also, Evaluating the effectiveness of a security program and try to avoid risks and hackers.

5. Gellis, H. C. (2004). Proctecting against threats to enterprise network security: Certified public accountant. *The CPA Journal, 74*(7), 76-77. Retrieved from http://mutex.gmu.edu/login?url=https://www-proquest-com.mutex.gmu.edu/scholarly-journals/proctecting-against-threats-enterprise-network/docview/212320978/se-2

This citation is helpful because it is talking about some threats to enterprise network security, On the contrary, it tells us the importance of encryption technology. Internet changes people's life. Information security become more serious. So, how to make protect against threats become more and more important.

6. Smid, M. E. (2021). Development of the advanced encryption standard. *Journal of Research of the National Institute of Standards and Technology, 126*, 1-18. doi:https://doi.org/10.6028/jres.126.024

This citation is helpful because it is talking about cryptographic algorithms. Strong cryptographic algorithms are essential for the protection of stored and transmitted data throughout the world.

7. H. Wang, G. Wang and L. Zhang, "Research on the Encryption of Ship-to-Shore Control Commands for Unmanned Surface Vehicle," *2022 7th International Conference on Automation, Control and Robotics Engineering (CACRE)*, 2022, pp. 8-13, doi: 10.1109/CACRE54574.2022.9834176.

This citation is helpful because it is talking about information security is used in development of Unmanned Surface Vehicle. In order to improve the information security, they used a hybrid algorithm that combines encryption. Also, they analysis the factors that can threaten the encryption of algorithms.

8. Lina Gong, Li Zhang, Wei Zhang, et al. The application of data encryption technology in computer network communication security. AIP Conference Proceedings 1834, 040027 (2017); https://doi.org/10.1063/1.4981623

This citation is helpful because it is talking about Symmetric key encryption technology and Asymmetric key encryption technology. Also, it's talking about encryption and decryption and how it works. Some more advanced algorithm design make data more security.