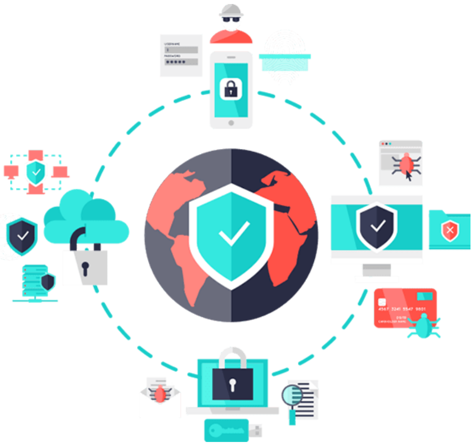
Network Security

Introduction

The ongoing rapid growth of computer network systems brings both a renaissance and a new security threat. Network security problem generally includes network system security and data security. In this paper, we go to learn what is Network Security, the Architecture of Network Security, the Objectives of Network security, the Practical uses of Network Security, and the Technologies of Network Security.

Network Security Definition



The common nouns related to computer security are network security, information security, information system security, network information security, network information system security, computer system security, computer information system security, etc. Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft. In short “Network Security” refers to the “CIA Triad”, which means C for confidentiality, I for integrity, and A for Availability.

.ITU-TX.800 standard defines the network security logically from three aspects:

- **Security Attack**: Network Security attack refers to the man-in-the-middle attack, Distributed-Denial-of-Service attack, which acts to damage the information, message change, damage the network traffic, etc.
- **Security Mechanism:** Network Security Mechanism refers to the detection and prevention of Network Security Attacks and system recovery. The different types of Security mechanisms are encryption, access control, data integrity, authorization, authentication, routing control, digital signature, etc.
- **Security Service:** Network Security Service assure the security aspects of any network. It includes the confidentiality, Integrity, and Availability of the network.

Network Security Architecture

Networking follows a five-layer TCP/IP model when it transmits any data from any end to another end. For the purpose of network security, we assure the security of every layer of the TCP/IP model.

- **Physical Layer Security:** Prevent the damage to data, decrease the data transmission rate, and also prevent the attack on the physical path.
- **Data-Link Layer Security:** Assure the data transfer rate through the network from eavesdropping where to apply the technique of VLAN in LAN and data encrypted when communicating with WAN.

- **Network Layer Security:** Assure the network provides authorization services only for authorized users, thus guaranteeing the correct network routing. The IP address is also responsible for the network layer security.
- **Transport Layer Security:** The security of information when it is transmitted from one end to another end is ensured by Transmission Control Protocol or TCP. It is a connection-oriented protocol. The data security is also assured by flow control and error detection in this layer.
- **Application Layer Security:** Application Layer Security refers to the both security of the operating system and the application system. Operating System security is assured by operating system access control & application system security is assured by communication content security, both sides of communication authentication and the auditing system.

Network Security Objective

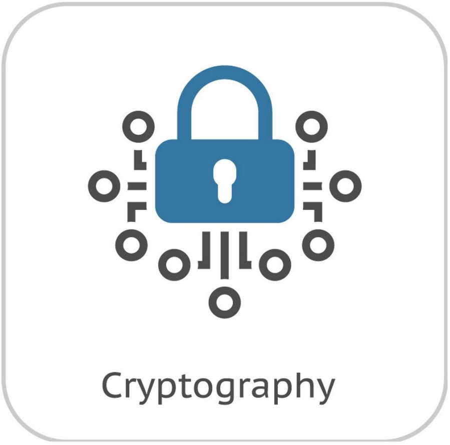
The objective of network security is to maintain confidentiality, authenticity, integrity, dependability, availability, and audit-ability.

Network Security Technologies

☐ **Authentication Technology:** Authentication refers to the authenticity of the entity. Authentication is based on cryptography, including identity authentication, message authentication, access authorization and digital identification.

1) **Identity Authentication:** It recognizes the user identity by authentication, which is always before allowing users access to the network resources. “Username&password” is the most commonly applied method.
2) **Message Authentication:** In order to guarantee the authenticity of the message source, private-keys of the both sides of communication can be applied to construct the message identification information.
3) **Access Authorization:** Access authorization refers to confirm the user access authority to the information resources after identity authentication.
4) **Digital Signatures:** Digital signature is mainly to prevent the impostor, and to ensure that the receiver can prove the authenticity of the message received and the sender to a fair third-party

□ **Data encryption Technology:** In the network security technology, data encryption technology is mainly to improve data confidentiality and prevent them from decoding. There are two types of encryption and that is symmetric-key encryption and asymmetric-key encryption.



1) **Symmetric-Key Encryption:** Symmetric-key encryption is also called as private-key encryption or single-key encryption. It applies the same key to encrypt and decrypt the message, which is shared by both the sender and receiver.
2) **Asymmetric-Key Encryption:** Asymmetric-key encryption is also called public-key encryption, which applies a public-key and a private-key. The message encrypted by the public-key can only be decrypted by the matching private-key.

□ **Firewall Technology:** Firewall is a security system between the internal network and the external network, which is used to strengthen the access control between networks.

Basic Functions of Firewall

- Filter the data packets that pass through the network;
- Manage the access behaviors pass through the network;
- Plugging some forbidden access behaviors;
- Record the information content and activities pass through the firewall;
- Detect and alarm the network attacks.

- □ **Intrusion Detection System:** An intrusion detection system is a kind of active network security technology, which is a reasonable supplement to a firewall. It collects information actively from the internal system and various network resources and analyzes the possible network invasion or attack.

- □ **Virtual Private Network (VPN):** VPN describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in real-time. In this case, tunnel protocol is used for the virtualization. Through the VPN the data is encrypted so the security is assured.

Conclusion

The computer network is the most powerful & useful tool for the technical area. It improves the system efficiency and reliability through distributed processing and also has good scalability. On the other hand, It is true that the security issue nowadays in computer networking into a threat. So, it is very challenging for us to maintain network security. As we need to be more aware of network security.

References

Citation Map

1. F. Yan, Y. Jian-Wen and C. Lin, "Computer Network Security and Technology Research," 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation, 2015, pp. 293-296, doi: 10.1109/ICMTMA.2015.77.

URL:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7263569&isnumber=7263490

2. G. A. Marin, "Network security basics," in IEEE Security & Privacy, vol. 3, no. 6, pp. 68-72, Nov.-Dec. 2005, doi: 10.1109/MSP.2005.153.

URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1556540&isnumber=33104