CHOOSING OPTIMAL METHODS AND PROTOCOLS FOR PROTECTING INFORMATION IN COMPUTER NETWORK

Yanko A., Krasnobayev V., Martynenko A., Horban V.
Poltava National Technical Yuri Kondratyuk University, Poltava, Ukraine

Prior to the advent of personal computers and computer networks, books, phones, telegraphs, and more were the primary means of messaging. But now, information technology plays an important role in the lives of each of us. With the advent of computer systems and global information and telecommunications networks, there are also issues such as protecting information from intentional unauthorized access [1]. The problem of information security is a particular concern for military or government agencies, as they may have secret information. The disclosure of such information could have resulted in enormous casualties, including human casualties [2]. Development of computer technologies allows to build networks with the distributed architecture. Therefore, a large number of network segments may be combined, which may be at a considerable distance from each other. Increasing the number of segments in a network also causes an increase in the number of network nodes and the number of lines of communication, which in turn increases the risk of unauthorized access. The specifics of information security in computer systems is due to the fact that the information is not rigidly connected with the carrier. Modern information can be easily and quickly copied and transmitted via communication channels [3]. There is no single technical means or method to solve these and other similar problems. But common in many of them is the use of cryptography.

The purpose of the paper is to study protocols and mechanisms for protecting information in computer systems and networks. The analysis of perspective directions of development of cryptographic encryption for ensuring confidentiality, authentication and integrity of information. The basic mechanisms that ensure the integrity and confidentiality of information are considered. Interception protection requires the use of additional protocols that support data encryption and authentication of data subjects. SSL/TLS (Secure Socket Layer/Transport Layer Security) protocol, which implements encryption and authentication between the transport levels of the receiver and the transmitter, is used to solve this problem [4].

References

1. Davis Peter, Lewis Barry. Computer security for "dummies".: 1997. – 272 p.
2. William Stallings. Network security basics. Applications and standards: Per. from English – M.: Williams Publishing House, 2002. – 432 p.
3. Richard E. Smith. Authentication: from passwords to public keys. : Williams Publishing House, 2002. – 432 p.
4. Cisco Network Admission Control (NAC) Solution Data Sheet // Cisco. January 23, 2017. URL: https://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean-access/product_data_sheet0900aecd802da1b5.html