Neo Science Peer Reviewed Journal
Volume 16, December 2023 ISSN (E): 2949-7701
www.neojournals.com

==========

THE PRIORITY TASKS OF ENSURING THE SECURITY OF THE COMPUTER NETWORK

Sultanova Dildora, daughter of Ilhomjon,
Teacher of the Department of Information Technologies,
Andijan Mechanical Engineering Institute

Abstract:

Conduct scientific research in key areas such as computer theory, computer science, data management and information measurement and analysis, network external and internal management, programming, data storage and management, production and management, etc. It is comprehensive in the scientific field it includes.

Keywords:

Encryption, protocols, identification, authentication, network viruses, Auditing.

Introduction

Computer throat _ _ theory computers and in them programs , protocols , network models , information measurements _ _ and management the basics learns _ _ _ In this area, how information is stored, how it is used and managed, how information is controlled from outside and inside organizations, etc.

Security is a field that includes a number of ways to ensure secure storage, transmission, and management of data and networks in computer systems. The main purpose of security is to control the existing security permissions in computer systems, to detect and delete malicious programs, to encrypt data, to provide an authentication and authorization system for users and system administrators, and to implement such important processes as others. Computer hardware is an essential tool for using, maintaining, storing, and communicating with computers. Through the computer network, we can store data, run programs, use the Internet, send e-mails, communicate on social networks, and more.

Computer security is one of the important guidelines for ensuring the security of computer systems, the information stored on them, and the security of their users. Security includes protecting computers against malware, hackers, attacks, and unauthorized access to information. The main tasks of computer network security are:

1. Computer and network security: The main task of security is to secure the systems on the network and computers. Since there are many aspects of security, it can be done by experts or security systems.

This is due to many security issues such as viruses, malicious users and closed/exploited logins. To ensure security, it is very important to use computer network monitoring and anti-malware protection systems. In addition, the methods of storing users' passwords and login information are also important factors in ensuring security.

==========

2. Data protection: Data, documents and all information stored in network systems must be protected against external transfer during document or system operation or only during storage. Security systems and new, advanced encryption algorithms are used for this purpose.

Data protection is an important component of security. This includes the direct protection of users and user data, controlling the absence of data and ensuring that no one is denied access to the data of fraudulent users. .

Data protection is one of several additional network security steps. This includes additional ways to secure systems such as data encryption, identifying and banning rogue users, data migration, and more.

Data protection prohibits the necessary rights to access the data of many types of users. Such rights, such as passwords, authentication in the form of biometrics, etc., are used to prohibit access to data protection systems.

Other additional features of data protection systems include:

- Data Self-Encryption: This is an important part of ensuring security in systems through data encryption. This method prohibits the identification of false users and the modification of data.
- Antivirus programs: These programs are used to detect and remove viruses on networks and computers. These programs are one of the main steps to ensure data protection.
- Prohibition of use of insecure networks: Insecure users may appear on the network. It allows you to block the access of users on the network to ensure data protection.
- Data Storage: Security is applied against data write and read vs. transfer.

3. User identification and authentication: Users must enter their ID and password when accessing the systems. Security systems must verify, encrypt and authenticate the user's identity and password.

User identification and authentication refers to verifying and verifying the identity of a user. Identification refers to determining the identity of the user, while authentication refers to confirming the identity of the user.

User identification is used to identify the user. In doing so, a username, password, ID number or other identification information is entered. This information is entered by the user when logging in and the system is stored in order to recognize the user.

Authentication is the process of confirming a user's identity. This is the next step in user recognition by the system. In doing so, the system must obtain the user's identification information and check the similarity between them to identify the user. For authentication, users are usually provided with a password or other authentication method.

User identification and authentication are important for network security. With these processes, it is determined that rogue users should not be allowed into the system. Also, the user's data is kept confidential and secure.

4. Ensuring Virus-Free: Viruses create many security problems in networks and computers. Therefore, the priority tasks of virus-free security are to find, hide, secure and remove the virus from the network.

Includes virus protection systems, advanced encryption and verification algorithms, certain data filtering and application data learning and compliance data learning.

In fact, viruses can cause many security problems in networks and computers. Viruses can cause widespread security problems with users' personal information on the network and connections between users. Viruses copy the information of users on the network and other systems on the network by sending files such as translations, notes, pictures and music of users to other users. Viruses attempt to obtain and use personal information and can be harmful to computer systems and users.

To ensure virus-freeness, it is recommended to follow the following tips:

- Store data and files only when and where users need them;
- Check before opening e-mails, e-mails or files sent directly to users;
- Using antivirus programs to scan files or messages while sending data;
- Installing and regularly updating antivirus programs on users' computers;
- Keeping automatic backup copies of user data, especially critical data, used in the implementation.

These tips help reduce viruses and other security issues and help protect users from security risks on their computers.

5. Auditing: Monitor computer systems, documents and user activities. This is called an audit. Auditing includes system migration, review of user activities, and detection of errors and security issues in systems and data protection systems.

Auditing is the process of monitoring, verifying and controlling the activities of computer systems, documents and users. This process helps to ensure the security of computer systems and identify errors, omissions and errors between systems and documents.

Some important indicators related to computer systems monitoring are:

- Ensuring the security of systems;
- Tracking active users in systems;
- Storing and studying the history of actions performed in the systems;
- Identification, analysis and correction of errors in systems.

System administrators or security experts are usually used in the auditing process. They are given the necessary capabilities, technologies and methods to monitor and secure the system.

Auditing is critical to computer systems because it is necessary to ensure security, data protection, and system performance quality. Inspections carried out by auditing help to identify errors in systems and documents and find solutions to them frequently and effectively.

6. Translation: Computer translation is one of the important means of ensuring the security of new records and encryption.

This includes the translation of simple texts and specialized records using translation systems widely used in international computer networks and the Internet to facilitate the exchange of large amounts of information.

These systems have encryption and decryption functions that allow text, files and other data to be transferred securely. The most common methods of encryption include asymmetric and symmetric encryption, hash functions, and other security protocols.

Computer translation is important because it provides a great service in our country and in the world, in our computer networks and on the Internet, for reading, translating and exchanging messages of other languages and nationalities. Therefore, computer translation and security is very important and a great need for all users.

Information security in the network is a common concern for network users' data and networked systems. Lack of security leads to loss of data, using networked systems and connections to them.

Information security in the network causes mistrust of our information, including personal and commercial information, emotional manipulation, access to personal information and other issues necessary to ensure security.

To ensure network security, it is necessary to use high-performance systems, protocols and solutions in the field of security. These protocols include the necessary technologies to ensure security for systems on the network, protect personal data, identify and solve security problems.

Information security in the network is one of the most important issues of the present time, and it is necessary to use high-performance systems and solutions that include the necessary security measures for users and systems in the network. These network security solutions and systems help better manage the network security situation, ensure security for network data, and help users maintain security for network systems.

References

1. Begbutayev AE Use of simulated virtual simulators in evaluating the performance of laboratory work. "Public education" scientific and methodical journal. #4. Tashkent-2019 - pages 57-63
2. Begbutayev AE Methodology of teaching the discipline "Network technologies" based on smart-technologies. European Journal of Research and Reflection in Educational Sciences. Vol. 7 No. 12, 2019
3. 7 (12), ISSN 2056-5852 Progressive Academic Publishing, UK. Pages 741-755
4. Begbutaev AE. Using simulation models in the study of computer networks. Eastern European Scientific Journal (ISSN 21997977) DOI 10.12851/EESJ201805 AURIS Kommunikations-und
5. Verlagsgesellschaft mbH Düsseldorf – Germany. 2019. 420-425, No. 2

6. Carpenter JP, Green Tim D. Mobile instant messaging for professional learning: Educators' perspectives on and uses of Voxer//
7. Teaching and Teacher Education. - Volume 68, November 2017, Pages 53-67. https://doi.org/10.1016/j.tate.2017.08.008
8. Chory RM, Offstein EH "Your professor will know you as a person". Evaluating and rethinking the relational boundaries between faculty and students // Journal of Management Education. - 2017. - Vol.
9. 41, Issue 1. – P. 9–38. DOI: https://doi.org/10.1177/1052562916647986
10. Computing//International Journal of Multimedia and Ubiquitous Engineering Vol.8, No.6 (2013), pp.313–328
11. http://dx.doi.org/10.14257/ijmue.2013.8.6.31
12. De Domenico, M. & Biamonte, J. Spectral entropies as information-theoretic tools for complex network comparison. Phys. Rev. X 6, 041062, https://doi.org/10.1103/PhysRevX.6.041062 2016
13. 16. Debbita Tan Ai Lin, Ganapathy, M. Manjeet Kaur. (2018). Sooo! It: Gamification in Higher Education. Pertanika Journal of Social Science and Humanities. https://www.researchgate.net/publication/320182671