

Analysis of encryption and authentication methods in wireless networks

Vinnytsia National Technical University

Abstract

In this work, the primary encryption and authentication methods used to protect wireless networks are examined, their advantages and disadvantages are analyzed, and their effectiveness is evaluated based on practical data. The prospects for further application are considered, and conclusions are drawn regarding their feasibility and effectiveness in practical use.

Keywords: computer networks, encryption, wireless networks, security, protocols, network traffic.

Анотація

У цій роботі розглянуто основні методи шифрування та аутентифікації, що використовуються для захисту бездротових мереж, проаналізовано їх переваги та недоліки, а також оцінено їх ефективність на основі практичних даних.

Було розглянуто перспективи щодо подальшого застосування, зроблено висновки щодо їх потрібності та ефективності у практичному використанні.

Ключові слова: комп'ютерні мережі, шифрування, бездротові мережі, безпека, протоколи, мережевий трафік.

Introduction

Security in computer networks plays a very important role in ensuring confidentiality and access to data. Wireless networks are particularly vulnerable to unauthorized attacks due to the easier possibility of detection and access. There are many methods and technologies for securing wireless networks that can help protect them.

Encryption and authentication methods

Traffic Wireless network security methods are the processes necessary to ensure security against unauthorized access to a wireless network, to ensure the security of data transmitted over a wireless connection, and to protect this data from unauthorized access. One of the ways to protect a wireless network from unauthorized access is to use wireless security protocols such as WEP, WPA, and WPA2[1]. These and other protocols have different encryption methods, standards, and algorithms, they provide user authentication and encryption of data transmitted between devices and access points, which allows you to ensure data confidentiality and prevent unauthorized access to the wireless network.

Device filtering methods on a wireless network are methods for the process of controlling or restricting device access to the network. One way to filter devices on a network is MAC address filtering, which allows only those devices whose MAC address is in the allowed list to access the network, and the advantage of this method is that it is easy to implement and configure, but the disadvantages of this filtering include the vulnerability to spoofing the MAC address on devices, where it is possible to spoof a desired MAC address and gain access to the network. Another way to filter devices on the network, for example, is IP address filtering, which works in a similar way to MAC address filtering, but it restricts access by device IP addresses[2]. You can also use 802.1X authentication, which has a high level of security among its advantages, which is achieved by verifying devices or users by their credentials, but the disadvantage is that this method requires setting up an authentication server, additional servers and infrastructure[3].

Access control and packet filtering is the process of securing a network by monitoring and controlling traffic. One way to implement this method of access control and packet filtering is to install and configure a firewall that will monitor and control all incoming and outgoing traffic, allowing or denying it to enter the network[4]. The process of protection is that only a firewall can restrict access to the internal network, allowing only authorized devices to transmit data, which is a plus, but the disadvantage is that they are difficult to configure, and certain types of firewalls have filtering limitations. There are two types of firewalls: software and hardware. Software firewalls are installed as software and are used as an additional

method of traffic control. Hardware firewalls are devices that are usually connected between the network and the external Internet, controlling all outgoing and incoming traffic.

Conclusions

Wireless network security is an important process that allows you to ensure confidentiality and security in a computer network, prevent unauthorized access and leakage of confidential information.

It is also important to consider the technical characteristics of the network to choose the most appropriate method of protection. For example, smaller networks may use simpler filtering methods that are easier to set up, software firewalls that are easier to maintain, and new technologies and security methods that can be used in current or new networks will be created in the future.

REFERENCES

1. Common Security Protocols for Wireless Networks: A Comparative Analysis [Electronic resource]. – Access mode: https://www.researchgate.net/publication/354887719_Common_Security_Protocols_for_Wireless_Networks_A_Comparative_Analysis
2. A Review of IP and MAC Address Filtering in Wireless Network Security [Electronic resource]. – Access mode: https://osf.io/preprints/inarxiv/g6emr_v1
3. Understanding and Configuring 802.1X Port-Based Authentication [Electronic resource]. – Access mode: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dot1x.pdf>
4. Network Security Using Firewalls [Electronic resource]. – Access mode: https://www.researchgate.net/publication/38112085_Network_Security_Using_Firewalls

Магас Людмила Миколаївна - старший викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, м. Вінниця.

Кубенко Денис Михайлович - студент групи 2СП-21б, Вінницький національний технічний університет, м. Вінниця, e-mail: denuskubenko1@gmail.com

Liudmyla M. Magas — Senior of English, FL department of Vinnytsia National Technical University, Vinnytsia.

Denys M. Kubenko — student of group 2SP-21b, Vinnytsia National Technical University, Vinnytsia, e-mail: denuskubenko1@gmail.com