ОГЛЯД СУЧАСНИХ МЕТОДІВ МЕРЕЖНОЇ СТЕГАНОГРАФІЇ

Анна Щербак, Марина Шаповал, Дарраж Муад
Науковий керівник – проф. Журавка А.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-20)

An object of study is a process of stenographic information hiding, which counteracts the threat of unauthorized access to it.

A subject of the research is network steganography methods based on changes in header and data fields in protocols.

An aim of the work is to research and implement network steganography methods, with special emphasis on consideration of quality assessment indicators of stenographic methods. Choose a method that could be used to improve the system of remote user authentication in communication channels by increasing the resistance to cracking and noise immunity of the system.

Steganography is a science that studies ways and methods of hiding the existence of sensitive information when stored or transmitted to prevent third parties from discovering it. The hidden information is called a transcript. They are located in a specific medium. In network steganography, the role of the carrier is performed by a packet transmitted over the network. There are two mandatory requirements for stenographic transformation: invisibility and reliability (resistance to distortion of all kinds). In addition, when constructing a stenographic system, the following provisions should be taken into account [1]: acceptable computational complexity of the steganosystem implementation; providing the necessary bandwidth; ensuring the authenticity and integrity of the hidden message for the authorized person; the potential offender knows all about the steganosystem and its implementation except the key; if the fact of the existence of the hidden message becomes known to the offender, then it should not be possible to extract it until the key is known.

An important factor is also the choice of the most favorable media for hidden messages in communication networks. Consider the basic requirements that they must meet.

1) They should be popular, that is, the use of the media themselves should not be considered an anomaly. The more popular media present and used on the network, the better because they mask the existence of a hidden connection.

2) Their modification associated with the introduction of the steganogram should not be visible to a third party who is not aware of the existence of a hidden link.

The use of network steganography is that it does not rely on the deception of the human sense, as it does when using methods of steganography that conceal data in digital images, audio and video files. Let's look at three groups

into which methods of network steganography are divided [2]. 1) Steganography methods, the essence of which is to change the data in the network protocol header fields and in the payload fields; 2) Steganography techniques that change the structure of packet transmission, for example, change the sequence of packet transmission or deliberate introduction of packet losses during their transmission; 3) Hybrid methods of steganography - when used, the contents of the packages, the delivery time of the packages and the order of their transfer change. In turn, some of these methods are divided into several groups. Packet modification methods include three different subgroups. 1) Methods for changing data in the protocol header fields. They are based on modifications to the IP, TCP, Stream Control Transmission Protocol (SCTP) header fields, and more; 2) Package payload modification methods. In this case, various algorithms for watermarks, language codecs and other steganographic techniques for hiding data are used; 3) Mixed techniques. Methods for modifying the packet transmission structure also include three directions. 1) Methods in which the order of packets is changed; 2) Methods that change the delay between packets; 3) Methods, the essence of which is to introduce deliberate loss of packages by omitting sequence numbers from the sender.

Thus, the general information on network steganography is reviewed and particular attention is paid to the fact that there are mandatory requirements for stenographic transformation, such as invisibility and reliability. Also, it has been found that an important factor is the selection of the most favorable media for hidden messages. To implement network steganography, it is planned to consider software that uses Transmission Control Protocol (TCP), Internet Control Message Protocol (ICMP), and Hypertext Transfer Protocol (HTTP) and network snippets to hide data on the network. These methods are planned to be compared by characteristics such as performance, efficiency, noise resistance and detection resistance. These characteristics make it possible to fully evaluate the effectiveness of the methods considered. The considered methods of steganography make it possible to successfully solve the problem of protecting information from unauthorized access.

References:

1. Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures / [W. Mazurczyk, S. Wendzel, S. Zander et al.]. – Hoboken: Wiley-IEEE Press, 2016. – P. 296.

2. Handel T. G. Hiding data in the OSI network model / T. G. Handel, M.T. Sandford II // Information Hiding: First International Workshop Cambridge / T. G. Handel, M. T. Sandford II., 1996. – P. 23–38.