Maksym Baranovskyi
A.A. Kuznetsov, research superviser
T.I. Titarenko, language adviser
Kharkiv National University of Radioelectronics, Kharkiv

Covert Channel for Cluster-based File Systems Using Multiple Cover Files

In computing, file systems are used to control how data is stored and retrieved. Without a file system, information placed in a storage area would be one large body of data with no way to tell where one piece of information stops and the next begins. By separating the data into individual pieces, and giving each piece a name, the information is easily separated and identified. Taking its name from the way paper based information systems are named, each piece of data is called a "file". The structure and logic rules used to manage the groups of information and their names is called a "file system".

There are many different kinds of file systems. Each one has different structure and logic, properties of speed, flexibility, security, size and more. Some of them found application in steganography – the branch of cryptography which task is to hide information in the way it would be unknown for unauthorized person that such information even exists. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny.

Our interest in steganography is to close security holes, which may appear in some cluster file systems. Data storages generally are rigid magnetic discs, divided into sectors and clusters – a cell in which the recorded information is stored directly. Data is stored in memory in the form of files, but the files themselves are not something indivisible, they split into pieces and scattered to different clusters of the carrier. The basic idea of the method of embedding data is to use multiple pre-selected files (cover files) and to hide the secret message with the relative positions of the clusters of the files relative to each other. Secret key in this case are the names of used files, the order of clusters of different files to each other and other features. These parameters need to know the recipient to retrieve information.

This method of hiding data has both advantages and disadvantages. The main advantage of the method is the high level of reliability (stealth) of such steganographic systems. Program analyzers, designed to search for hidden embedded information cannot detect the hidden message because does not change any data bit. The disadvantages are, primarily, vulnerability to defragment, which will destroy all the hidden data.

In this study were analyzed new data channels, identified their strengths and weaknesses, which will close some security holes and improve the reliability of computer systems.