UDC 004.056.5 (043.2)

Myronenko O. K.
National aviation university, Kyiv

MONITORING OF NETWORK ACTIVITY OF PERSONAL COMPUTERS ON THE BASIS OF AGENT TECHNOLOGY

The last years brought substantial changes in solutions of problem of access defence to the resources of corporate network. Yet quite recently it was possible to provide security of the information systems with the high degree of reliability by such traditional measures as authentication and authentification, access differentiation, encryption, et cetera. However, with introduction and development of the open computer networks the situation changed sharply. The results of researches indicate that most companies with corporate networks utillize such systems of defence as inter-network screens, anti-virus programs, intrusion detection systems (IDS). According to the CSI/FBI reports, there are new trends in providing of information security. Companies began to spare attention to both the systems for logging security events and automated systems activity, and systems which allow to conduct the analysis of events (at investigation of incidents).

Sniffer (traffic analyzer) is a network analyzer of traffic, programmatic or software-hardware device, intended for interception and subsequent analysis, or only analysis, of network traffic, intended for other sites.

As it is known, interception of traffic can be carried out in the following ways:

- ordinary «listening» to the network interface (a method is effective while using the concentrators (hubs) segment of LAN instead of switchboards; otherwise, a method is ineffective, as sniffer gets only separate frames;
- connecting the sniffer in the break of channel;
- by branching (programmatic or hardware-based) of traffic and direction of its copy on sniffer;
- through an attack at the channel level (MAC-spoofing) or at the network level (IP-spoofing), which results in redirecting of traffic to the sniffer with its subsequent returning.

Analysis of traffic which passes through the sniffer allows:

- to find out a parasitic, viral and circular traffic, the presence of which increases the load of network equipment and data channels;
- to find out harmful and unauthorized software in the network, for example, network scanners, flooders, trojan programs, clients of peering networks et cetera.
- to intercept any uncoded (and, sometimes, also encoded) traffic of user.
- to localize the disrepair of network or error of configuration of network agents.

In order to provide the permanent monitoring of network traffic, even in the situations with the failure of equipment and at impossibility of intervention from an administrator, there is a requirement in more intellectual system, which would be able to make an independent decision in accordance with the situation.

Development of the system of monitoring of network traffic of the personal computers on the basis of agent technology will allow to provide more reliable informative security of corporate network of organization.