COMPUTER NETWORK TRAFFIC MANAGEMENT SYSTEM

Tojiyeva Feruza Qobiljon qizi
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan

Annotation: Implementation of a self-organizing traffic management system for a computer network based on the presented methods involves the use of certain tools and includes three main blocks: forecasting and falsification of server solutions, and corporate servers. The results of experiments on identification of security systems and vulnerabilities (through scanning and probing mechanisms), decryption of internal information flows of the enterprise's local computer network, and resistance to distributed network attacks (including denial of service) in a comparative analysis with existing solutions are presented. The proposed methods of ensuring information security have shown high efficiency and stability.

Keywords: information security, traffic management, genetic algorithmization, network activity

Introduction

The need to protect information processes and procedures for their electronic automation is one of the priorities of modern IT technologies. Today, major crimes are committed, including using the global Internet. Almost all state structures and private organizations have access to this network, protecting their information flows with firewalls, cryptographic tools and anti-virus software that operate on the basis of "hard" logic. However, at a certain time cost and computing power, any information system can be hacked or removed from the availability state [3]. By using scanning, probing, and decryption mechanisms, an attacker can identify the security product of the attacked object, as well as get a list of vulnerabilities of the object with information on their use. The vulnerability of the TCP/IP Protocol stack and the programmed "hard" logic of various hardware and software tools for managing and protecting traffic make it necessary to support the information and communication technology sector of the enterprise with qualified technical specialists. Another factor in

ensuring information security is the potential possibility of finding an attacker from among trusted users of the corporate network, including from the staff of IT specialists.

The purpose of this work is to develop methods that will form the basis of a self-organizing traffic management system for a computer network [2].

The key task is to develop methods for countering network threats and ensuring the confidentiality of information flows in distributed enterprise-level computing networks.

The scientific novelty of this work consists in the development of methods and self-organizing traffic management apparatus of the computer network, which has the properties of dynamic adaptation, optimization, autonomy, fault tolerance of the highest class and provides a high level of information security with the possibility of predicting the response strategy. The essence of the proposed approach is described in this paper.

I. Method of countering network threats. When developing enterprise-level computing networks, we suggest using the following method of countering network threats, using the apparatus of genetic algorithmization and fuzzy logic, which involves the sequential execution of the following operations:

1. Initial scan of the network topology and configuration.

2. Configuring the basic rules of the traffic management system based on the current security policy.

3. Deployment of prediction and falsification blocks:

3.1. Installing and configuring isolated virtual servers.

3.2. Analysis of installed instances, for the firewall configuration files for imitating information systems is being prepared.

4. Installation of a response model for third-party SSU connections selected by the genetic algorithmization block [2] from the sample of clause 3.2 for a certain time interval (iterations after expiration).

5. Performance of dynamic signature analysis of traffic with identification of scanning, probing and hacking attempts. If suspicious network activity is detected, the threat level is assessed and the response is:

5.1. In case of a low level of threat, connect the genetic algorithmization block, which consists of three categories of roulettes (objects, groups, and classes of objects).

5.2. In case of a high degree of threat, the fuzzy logic block responds with falsification of the server solution: redirecting the connection to an isolated server model of a certain type, tracking further actions of the attacker. A similar method is used to simulate a "hang" state in order to detect malicious nodes.

6. Tracing and identifying malicious hosts and further blacklisting them with temporary blocking.

7. Systematic self-organization of the system with preliminary verification of solutions on its models.

The packet travels with step-by-step decryption, and only the last node de-encapsulates the packet definitively and passes the information over an encrypted channel (for example, https over a vpn) and runs the response along the same chain).

To minimize this possibility, the authors propose a method for ensuring the confidentiality of information flows in the corporate network, which is based on a distributed self-organizing encryption system. This idea appeared when studying the "onion routing" of tor networks [1] created for anonymization on the Internet. At the same time, the software basis and the principle of encryption are implemented in a more secure way.

This method includes the following steps:

1. In the virtual server block space a trusted corporate network certification authority (CA) is installed and configured.

2. Using group policies or "manually" on workstations, the client part is deployed;

3. Using fuzzy logic, the CA configures the Protocol for interacting with hosts within this corporate network, creates a list of trusted nodes, and synchronizes it with the client part;

Experimental result: One of the variants of a self-organizing traffic management system for a computer network based on the proposed approach was implemented and its performance was analyzed. For this purpose, more than iGG iterations of SSU scanning were performed (with the set parameter for the response of the falsification block up to 2G% to detected scanning processes) using the programs XSpider, LanGuard, Shadow Security Scanner, X-Scan with parallel use Of Gcodepro and Zond Guard probing tools in each iteration.

In parallel, during the year, an experiment was conducted to decrypt confidential data of the SSU network by implementing sniffers (CommView, IRIS, LanExplorer, Net Analyzer) in the communication channels of various branches, as well as channel-level traffic decryption tools (unMili-taryZ, BDUpro, and other specialized tools) on computing clusters of 15 DELL PowerEdge ™ R720 12th Generation DX290 servers (Dual Intel ® Xeon ® E5-2620 Hexa Core incl. Hyper-Threading Technology128 GB DDR3 ECC RAM optional max. 384 GB, RAID Controller Dell PERC H710 8 Port SAS/SATA 6Gbit/s, Redundant Platinum Certified Hot Plug).

Attempts to decrypt the data within the described time interval were unsuccessful.

In identical conditions of interaction between two hosts, the developed system is not inferior to i2p technology, winning functionally in the field of corporate computing networks.

Conclusion: Developed methods to counter network threats and information security corporate flows underlying the self-organizing system of traffic management have proven to be a reliable offline and failover protection in the ICT sector, excluding the possibility even predict the response strategy and decrypt information in a cost effective timeframe. The disadvantage of the system is the requirement for significant computing power, since the rest of the protection would be enough CPU Intel Pentium IV 4 GHz (or similar), RAM 1 Gb, HDD 30 Gb. Given that the development of microelectronics is rapidly gaining momentum, the requirement to provide the declared computing power is not a significant disadvantage.

Literatures:

1. Azhmukhamedov I. M. Dynamic fuzzy cognitive model of threat influence on information security of the system / / Security of information technologies. - 2010. - n. 2. - Pp. 68-72.

2. Basynya E. A. Intelektualno-adaptive methods of ensuring information network security / E. A. Basynya, A.V. Gunko / / Automation and software engineering. - Novosibirsk: NSTU publishing house, 2013. - Issue 3. - Pp. 95-97.

3. Basina E. A. prospects of development of cryptography / Basyna E. A., Frantsuzova G. A., Gunko A. V. // advanced science, engineering and technology: mater. III-th Intern.

Scientific-practical Conf.: in 3 vols. - Kursk: SWSU Publishing house, 2013. - Vol. 1. - P. 199-200.

4. Gamayunov D. Yu. Detection of computer attacks as a problem of image recognition / D. Yu. Gamayunov, A. I. Kachalin // Matera. It's All Over. Symposium on applied and industrial mathematics: Kislovodsk: TVP Publishing house, 2004, pp. 91-95.

5. Gunko A.V. Stochastic methods for ensuring information network security / XI international Conf. - Novosibirsk: NSTU Publishing house, 2011. - Vol. 7. - P. 47-49.