СЕКЦИЯ 3
ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

CORPORATE NETWORK SECURITY SIEM-SYSTEM IMPLEMENTED ON ZABBIX SOFTWARE

Al-Baiati Ali Emad, A.S. Shelkov, N.V. Nasonova

Security incidents and events monitoring systems (SIEM) play an important role in enterprise information systems. SIEM systems have one or more log servers that perform log analysis, and one or more database servers that store logs. Regardless of how the SIEM server receives log data (either agentless or agent-based), the server analyzes data from all sources, correlates events among log entries, identifies and prioritizes meaningful events, and initiates response to events, if necessary.

SIEM solutions usually make it possible to protect privacy, integrity, and availability of these logs. For example, communications between agents and SIEM servers usually pass through a reliable TCP protocol in encrypted form. In addition, agents and SIEM servers can use authentication before they can transfer the data (for example, sending data from the agent to the server, making server-side changes in the agent settings).

Zabbix software was studied to implement a SIEM-system for a corporate network. Among many well-known monitoring systems Zabbix monitoring system was chosen for the implementation of SIEM. The capabilities of this system make it possible to use it as a system for collecting information, for its further processing and detecting IS events and logs analyzing in various operating systems, for making a decision on the occurrence of an IS incident, for notification of staff members responsible for the IS system, and for response to the known threats in a preventive manner.

On the basis of the examined information on the Zabbix system and the capabilities of hardware virtualization, a laboratory model was created, on which the network attack and the Zabbix system response to it can be demonstrated. Depending on the hardware resources, the model can be expanded, which makes it a useful tool for the investigation of network attacks, the information system response to network attacks, and the SIEM-system testing on the basis of the Zabbix software.

MODIFIED RLE ALGORITHM FOR SATTILITE IMAGE COMPRESSION

H.K. Albahadily, V.Yu. Tsviatkou

New suggested RLE compression algorithm to compress satellite grayscale images and reduce the size of the encoded data by reducing the bits needed to represent the coded date with bitplane technique. The proposed methods achieved very good compression ratio with satellite large space images of earth. The modified RLE algorithm ISN using the same idea of RLE which counts repeated runs but – instead of reserving fixed size of bytes to save the repeat and runs as pairs – we will send the repeated runs with a value representing how many bits need to save that repeat [1].

So *I* representing the pixel value,*S* representing the variant size of how many bits needed to represent it and *N* is the repeated times. The results were very good as we can see in the table below.

Table of compression ratio for test images layers 8–5

Layer	Img1	Img2	Img3
L8	1.3641	1.5950	1.0902
L7	1.2788	1.3636	0.8284
L6	0.9224	1.0950	0.5899
L5	0.6123	0.6591	0.4933

The results showing that the modified algorithm ISN provides compression ratio up to 1.595 times for MSB layer according to the nature of the image and its bitplanes.

References

1. New modified RLE algorithms to compress grayscale images with lossy and lossless compression / H. Albahadily [et al.] // International Journal of Advanced Computer Science and Applications. – 2016. – Vol. 7, № 7.