THE MODEL OF DETECTION OF THE NETWORK INTRUSION

[1]Nikitina L., [2]Nyamu L.

[1]National Technical University «Kharkiv Polytechnic Institute», Kharkiv,
[2]Kharkiv National University of Radioelectronics, Kharkiv

In our days, network and computer security becomes very important problem. Now Lot of vulnerable systems are available to attackers. Attackers can employ a large number of vulnerable hosts to launch an attack. A distributed denial of service (DDoS) attack is a large-scale, coordinated attack on the availability of services of a victim system or network resources, launched indirectly through many compromised computers on the Internet [1].

DDoS defense schemes are of three types based on their deployment: source-end, victim-end and intermediate router defense mechanisms. We have used the victim-end approach.

In the known attack model [2], its assessing is based on severity:

Severity = Valnurability – CounterMeasures= (Criticality + Lethality) –
– (SystemCounterMeasures + NetworkCounterMeasures)

This model has to change its behavior depending on the dynamical conditions of networks and computational resources. Implementation of this model becomes an “intelligent” and adaptive by the application of fuzzy logic techniques.

The goal of our model is to assign a correlation probability to each component of attack severity and to use this probability to discover is severity value higher than the threshold. If it finds such situation, the alert message has to be sent to the system administrator.

Network events are checked against predefined rules or patterns of attack. In our approach, general representations of known attacks are formulated to identify actual occurrences of attacks. For every component of attack severity we have proposed collection of fuzzy rules with linguistic variables and membership functions that represent key characteristics or indicators in relating probability. Fuzzy rule matcher selects and applies appropriate rule and determines risk of possible attack and classifies it.

The designed model was simulated it in the Fuzzy Logic Toolbox of MATLAB. The designed fuzzy inference system allows estimate the influence of attack characteristics on its severity.

References

1. Kashyap, H. J. and Bhattacharyya, D. K. A DDoS attack detection mechanism based on protocol specific traffic features. Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, Coimbatore, India - 2012, 26-28 October, pp. 194–200. ACM.

2. Астахов А., CISA, 2002. Актуальные вопросы выявления сетевых атак [Электронный ресурс]. – Режим доступа: http://www.iso27000.ru/chitalnyi-zai/setevaya-bezopasnost/aktualnye-voprosy-vyyavleniya-setevyh-atak