Yadigar N. Imamverdiyev[1], Babek R. Nabiyev[2]
Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]yadigar@lan.ab.az, [2]babek@iit.ab.az
DOI:10.25045/jpit.v07.i1.04

QUEUING MODEL FOR INFORMATION SECURITY MONITORING SYSTEMS

A model of queuing is proposed for the modeling of incidents handling process in the information security management system. Incident handling process is described by the model of M/G/1, which is carried out as mixed-priority services, and analytic expressions of the average waiting time are given for three priority classes, which are the absolute, relative and without priority modes of service. The model is proposed for the evaluation of the efficiency of the performance of the processing of information security incidents by including the penalty functions, based on the characteristics of the probabilities.

Keywords: *information security, information security incidents, network traffic, monitoring, queuing theory, priority handling.*

Introduction

The rapid development of information technology in the globalized world, new network equipment and increased types of traffic content flow, and the management process of corporate network (CN) is becoming both complex and financially expensive process. It can be explained by the fact that, as a number of utilities demanding control and monitoring mechanisms increases, the monitoring process requires a large amount of computing power, and this in turn, challenges the CN's performance. The main goal of the CN's monitoring is to provide uninterrupted network performance, integrity and confidentiality of corporate data. Therefore, the incidents are detected by controlling the traffic flow in general. The efficiency of information security service (ISS) needs to be increased to control the process and ensure its maximum security within the allocated budget.

Information security monitoring ensures the acquisition of the data about the real-time status of CN's information security, its assessment, and the elimination of the identified cyber-attacks and resolution of other incidents with minimal cost and time. In this regard, the monitoring plays a leading role in ensuring information security, where effective organization of ISS's performance is of great importance.

Analysis shows that the main challenge here is the rapid growth of the number of information security incidents, and the limited human and technical resources at the disposal of the service. The effective distribution and management of these limited resources is very crucial for handling the various types of information security incidents. Taking this into account, queueing models are developed for the optimal selection of ISS's parameters in the case study. Models promise that the accidental flow of information security incidents enters into the system input from sensors (IDS, network monitor, log-file analyzers, user data, etc.). The handling time is random.

Queueing model of is widely used in the solution of the practical issues of the probability theory, and its various analytical and simulation models have been proposed in the scientific literature [1]. Queuing theory is widely used in telecommunication systems and has played a particular role in the development of scientific and methodological basis of the Internet [2].

Related Studies

In general, queueing theory (QT) can be used not only in the field of information technology, but also in any field dealing with the service delivery and queue sequence. Therefore, the studies based on QT have been tested and provided opportunity to obtain detailed information about them. The requests related to QoS performance optimization [3], network controlling, detection and prevention of DDoS attacks [4], network traffic prediction [5] and others are received through QT.

Hedayati et al. [5] shows the QT-based assessment of network traffic monitoring. Network security monitoring in corporate environment is very important, in terms of assessment of security

and effectiveness of the incidents occurring in the network. In addition, network traffic controlling, forecasting and its quality are argued. For network traffic control and load balancing, Little's Law is used. Therefore, more complete information about the status of network traffic is possible to be obtained basing on intelligent forecasting process.

Theorital tools can be utilized for network traffic management. For example, the IP protocol handles the extra load control process. In [6], the active queue control technology and linear observer of time delays for the traffic monitoring in TCP protocol are developed. More specifically, the study focuses on the long-term TCP connections passing through narrow straits and routers of network topology. The mechanism placed in the router allows network controlling, with regard to TCP flow assessment and defining the types of anomalies.

[7] studies the development of the base model for network traffic monitoring based on the Queueing System (QS). Here, network traffic loading can be predicted according to (M/M/1): ((C + 1)/FCFS) and (M/M/2): ((C + 1)/FCFS) models. Based on these models, we can acquire a stable formula for network traffic prediction and traffic jams.

In [8], the base model of monitoring data transmission process is reviewed as a queueing model. This approach is based on a simple queue, according to the monitoring process performed on levels 1-5 of the OSI model in the network structure. By realizing the M/M/1 queueing model, the formula for network traffic predicting routes and stable load rates were presented.

Network screens are used at CNs to manage external threats. This network screens check them in accordance with the traffic and may prevent certain threats. As it is known, if the specific remedial measures are not taken to prevent DDoS attacks, it may lead to a violation of availability of the systems and services. In [9], analytical queuing model based on the Markov chain is applied. Based on this model, productivity of the network screen, at normal time and when it is exposed to DDoS attacks, is analysed. As a result of experiments, the formulas and productivity indicators of the main features were obtained.

We propose various queueing methods that minimize the monitoring time and optimize online monitoring of the CN nodes within the allocated network resources. In [10], to achieve this goal polling system model is proposed, and as a result of its optimization the time spent for monitoring is minimized.

The M/G/1 Model for Information Security Incidents Handling

One of the main features of ISS is that information security incidents (QT orders) are received through various sensors (IDS, firewall screens, information security tools, applications and users) in real time, and it responses by handling each incident without service denial. Throughout the process, there is no time limit on the request consideration. Nevertheless, the penalty functions can be applied for the effective management.

Each information security incident received by ISS is given the priorities in the positive integers (1, 2, 3, ...) according to a set of criteria. The more number increases, the more priority reduces i.e. 1 - indicates the highest priority. For instance, ITIL approach to the incidents handling [11] defines a priority, by the scale of 1-5, according to the incident urgency (how quickly it is handled) and the degree of its impact. To define the priorities of the information security incidents the hierarchical criterion system and appropriate evaluation method is proposed in [11].

Based on the priorities, ISS organizes the incident handling. Critical incidents are treated as requests with an absolute priority, i.e., when such incidents are received the handling of low-priority incidents stops and the service personnel is directed to the definite-priority incident. It is supposed that the medium-priority incidents are handled as the relative-priority orders are processed. It means that when the relative-priority incident is received throughout the service process the current incident handling does not stop, and waits in the queue. Then the high-priority incident is selected from the queue.

Low-priority incidents are handled in the out of priority mode. The orders in the service in the mode without priority do not have the privilege to be served extraordinarily. They are served

in FIFD (First In - First Out), LIFO (Last In - First Out) or RAND (Random) modes. The dispersion of the mean waiting time of all these no priority service orders is minimal.

Application of the QT M/G/1 model is proposed to control ISS's performance in this case study. As it is mentioned in [12], these types of models are mostly used in data processing.

For example, a simple flow of orders with the intensity $\lambda_i, i = \overline{1,M}$ enters QS. QS is assumed to have a service channel (CERT team). These flows generate Poisson stream, the intensity of which is $\Lambda = \sum_{i=1}^{M} \lambda_i$. The distribution of the service time is assumed to be the general distribution. b_i – denotes the mathematical expectance of the service time of the *i*-th flow orders, and $b_i^{(2)}$ denotes the 2nd start moment. The loading generated by the QS's *i*-th orders is used as $\rho_i = \lambda_i b_i$.

The mixed-priority service order is selected for incidents handling procedure. In general, QS with mixed-priority service order is considered: the incidents in the range of $\overline{1,M_1}$ have absolute priorities, M_2 number of orders in the range of $\overline{M_1+1, M_2+M_2}$ have relative priorities, and the other M_3 number of the orders are handled in the out of priority mode.

Thus, three priority classes are considered. First-class orders have absolute priority compared to the second- and third-class orders, and the second class has relative priority compared to the third class.

We intend to find the mean waiting time of the orders of different classes of priority (information security incidents) in QS:

The mean waiting time of the absolute priority incidents is not dependent on the characteristics of the service. The mean waiting time, $w_k^{AP}, k = \overline{1,M_1}$ for these incidents, can be calculated with the following formula [1]:

$$w_k^{AP} = \frac{R_{k-1} b_k}{1-R_{k-1}} + \frac{\sum_{i=1}^{k} \lambda_i b_i^{(2)}}{2(1-R_k)(1-R_{k-1})} ,$$

Here $R_j = \sum_{i=1}^{j} \rho_j$ - denotes the total load, generated by the first flow of the priority *j* (i.e., high priority).

The first addend indicates the time spent in queue because of the service interruption due to the high-priority incidents.

Note that if *k* = 1, we obtain $w_1^{AP} = \frac{\lambda_1 b_1^2}{2(1-\rho_1)}$.

The mean waiting time, w_k^{RP} for the relative-priority incidents, can be determined by the following formula [2]:

$$w_k^{RP} = \frac{R_{M_1} b_k}{1-R_{M_1}} + \frac{\sum_{i=1}^{M} \lambda_i b^{(2)}}{2(1-R_{k-1})(1-R_k)}$$

Here, $k = \overline{M_1+1, M_1+M_2}$, $R_j = \sum_{i=1}^{j} \rho_j$.

The mean waiting time, w_k^{RP} for the incidents without out of priority mode, can be determined in a similar way [13]:

$$w_k^{WP} = \frac{R_{M_1} b_k}{1-R_{M_1}} + \frac{\sum_{i=1}^{M} \lambda_i b_i^{(2)}}{2(1-R_{M_1+M_2})(1-R)} \quad , \; k = \overline{M_1+M_2+1, M} ,$$

Here, $R = \sum_{i=1}^{M} \rho_j$ is the load generated by the total flow.

Assessment model for incident handling effectiveness

The proposed queueing model may also be used to evaluate the effectiveness of ISS. Proposed mass queueing model can also be used to assess the effectiveness of ISS.

Real-time operation of ISS is desirable (ideal), it should be appropriate to the speed of incident input. In practice, this means that information security incidents should be handled within certain limited periods: $T_{p_i} < u_i^*$, here, T_{p_i} denotes the response time of the system to the *i*-th type of incident, and u_i^* - is the permissible maximum period of existence of the *i*-th type of incident in the system.

We can review 3 cases of periods depending on the requirements:

1) no restriction on the service period;
2) mean restriction on presence and waiting period in the system (i.e., average fulfillment of requirements);
3) absolute restriction on presence and waiting period in the system (i.e., the requirements are fulfilled for each order).

Let's review the solution of the problem of assessing the effectiveness of handling information security incidents in the first case. Two parameters are used for evaluation:

- λ_i - speed of incident input, $i = \overline{1, M}$;
- θ_i and $\theta_i^{(2)}$ - mathematical expectation and the second start moment of the labor capacity of the *i*-th type of incident handling, and is characterized by the random distribution function.

Despite the restriction on the response period to the incidents, it is considered that the longer event remains; in the system, the more the quality of the system's performance reduces. The efficiency criteria of such system can be characterized by the following penalty function:

$$F = \sum_{i=1}^{M} \alpha_i \lambda_i w_i \ ,$$

Here, α_i - is the penalty coefficient, and determines the value of the delay of the *i*-th type incident handling. The delays, that is the time w_i, depends on two factors: the handling speed of service device and service procedure. Accordingly, it is necessary to minimize *F* for the optimization of the system.

When the response time is unrestricted, it is necessary to provide sufficient speed for the maintenance without rejection. Obviously, in this case, the system should operate in stationary mode R <1, that is, the handling speed should exceed the speed of input.

In the case of non-homogeneous incidents, the loading is as follows:

$$R = \sum_{i=1}^{M} \rho_i = \sum_{i=1}^{M} \lambda_i b_i$$

However, b_i is defined by the handling capacity of the incident and the service speed of the device: $b_i = \frac{\theta_i}{B}$, here, B – denotes the handling speed of the device. We found the boundary value of handling speed as follows:

$$B > \sum_{i=1}^{M} \theta_i$$

That is, in this case, the restrictions to the system are determined by the parameters λ and θ. The incidents may be ranked by their importance, i.e., they may have the certain coefficients α_i. If all information security incidents have the same ranks, then appropriate coefficients α_i will

be $\alpha_i = \alpha = const$, and the penalty function is simplified:

$$F = \sum_{i=1}^{M} \lambda_i w_i = L,$$

Here, L – denotes the total length of the queue in the system, and the quality of the system should be minimized in order to improve it.

Conclusion

This article proposes the M/G/1model for developing the process of information security incident handling, based on the Queueing theory. Information security incidents are received from various sensors in real time mode, and each information security incidents, entered the ISS, are given priorities according to certain criteria and processed in accordance with these priorities. The proposed model provides analytical expressions of mean waiting time to be handled in three major classes of information security incidents, which are absolute, relative and non-priority service modes. Throughout the process, there is no time restriction on the consideration of the requests. However, we propose a model including penalty functions with the use of probability characteristics obtained for effective management of performance.

References

1. Gnedenko B.V., Kovalenko I.N. Introduction to queuing theory, M.: Publishing House of LKI, 2007, 400 p.
2. Kleinrock L. Computing queues: trln. from Eng. M.: Mir, 1979, 600 p.
3. Shikhaliyev R.G. On the methods of QoS monitoring and management of computer networks // Problems of Information Technology, 2013, No.1, pp.15-23.
4. Kumar S., Bhandari A., Sangal A. L. Comparison of Queuing Algorithms against DDoS Attack // International Journal of Computer Science and Information Technologies, 2011, vol.2, pp.1574–1580.
5. Hedayati M., Kamali S.H., Izadi A.S. Notice of retraction the monitoring of the network traffic based on queuing theory and simulation In heterogeneous network environment / International Conference on Information and Multimedia Technology, 2009, pp.396–402.
6. Ariba Y., Gouaisbaut F., Rahme S., Labit Y. Traffic monitoring in transmission control protocol/active queue management networks through a time-delay observer // Control Theory & Applications, 2012, vol. 6, no. 2, pp.506–517.
7. Saha Ray S., Sahoo P. Monitoring of network traffic based on queuing theory / National technology institute of Rourkela, 2011, pp.30.
8. Kammas P., Komninos T., Stamatiou Y.C. Queuing theory based models for studying intrusion evolution and elimination in computer networks/ Fourth International Conference on Information Assurance and Security, 2008, pp.167–171.
9. Yang W., Chuang L., Quan-Lin L., Yuguang F. A queueing analysis for the denial of service (DoS) attacks in computer networks // IEEE Transactions on Network and Service Management, 2011, vol.9, no.1, pp.12–21.
10. Shikhaliyev R.G. Improving the efficiency of the monitoring of computer networks based on the polling system optimization // Problems of Information Technologies, 2015, No.8, pp. 576–584.
11. Jan van Bon (ed.). Foundations of ITIL V3. 1st edition. Van Haren Publishing, 2007, 350 p.
12. Khrustalev Yu.P. Modelling of queuing systems. Irkutsk State Technical University, 2007, pp. 116.
13. Imamverdiyev Y.N. An information security incident prioritization method / 7th Int-l Conf. on Application of Information and Communication Technologies (AICT'2013), 09-11 Oct. 2013, Baku, pp.183–187.