Acta Technica 62 No. 2B/2017, 341–350

Hierarchical protection mechanism of network information based on computer security model algorithm terminal

Yue Peng[1], Zhao Limin[1]

Abstract. With the continuous development of computer communication technology, people's life, work and other aspects have undergone major changes, and have become more and more dependent on the network information. At the same time as the network information continues to increase, the increasing demand for its security has become the focus of its research. Therefore, the research and implementation of hierarchical protection mechanism for network information based on computer security model algorithm terminal was proposed. Through the construction of the computer security model, the computer terminal network information was hierarchized and protected. The experimental results show that the protection mechanism can effectively classify the network information and effectively protect the network information.

Key words. Computer security model, algorithm terminal, network information level, protection mechanism.

1. Introduction

With the continuous development and popularization of computer communication technology, people's lives, work and other aspects have been inseparable from the network, and the network has brought convenience to people's lives and work. However, with the continuous increase of network information, its security problems become increasingly prominent. In order to be able to provide users with better security services, the concept of security platform has been widely extended and widely used. The protection measures are mainly for the protection of the platform outside, if the back of the platform is entered, there is no difference in its grade [1]. It is precisely because of this, that seemingly safe protection is actually very fragile, once someone enters the security platform inside, its security does not make any sense. Therefore, how to protect the network confidence has become a hot topic in

[1] College of Management, Xinxiang Medical University, Xinxiang, Henan, China, 453003

the field of computer and the community [2]. Our country has a large population, although the level of computer development is still a certain distance from the international level, China's Internet users have reached 100 million, ranking first in the world. This also means that people enjoy the convenience and favorable information brought about by the network, at the same time, the demand for the protection of network information is growing, so China needs to strengthen step in this respect.

2. State of the art

Since the advent of the information age, all countries in the world have strengthened their investment in network information security, and have continuously researched and widely applied the technology of network information security protection, so that a series of security concept and corresponding protection methods have been formed, and a number of network information security management and protection systems have been established. For example, the United States has proposed Protection of Critical Infrastructure in the United States, and has carried out a number of organizations for the establishment of information security, including the National Information Security Committee, the Chief Information Officer Committee and the Federal Computer Event Response Action Group and other more than 10 national institutions and organizations [3]. Subsequently, the US National Security Agency developed the Information Security Technology Framework based on the actual situation and future needs, and proposed the "deep defense strategy" concept, determined the goals of network and infrastructure defense, as well as the defense of environmental defense and supportive infrastructure [4].

Our country started relatively early in the construction of network information security. The state has made great efforts to support and promote the construction of this aspect. After several years of efforts, our country has achieved relatively good results, and the network information security technology has been rapidly developed and applied [5]. For example, the Regulations of the People's Republic of China on Computer Security Protection formulated by the State Council of the People's Republic of China stipulates that the computer information system should carry out security grade protection, and carry out the management through the security of network information classification standards and classification management related measures, in addition, the Ministry of Public Security in conjunction with relevant departments should formulate the standards for the classification of grades and the measures for their administration. At the same time, the Opinions of the National Informatization Leading Group on Strengthening Information Security Work forwarded by the general office of the Central Committee and the general office of the State Council clearly illustrates the importance of network information management, information classification and related management measures [6].

2.1. Methodology

Hierarchical protection of network information is the rational classification protection and the guidance of classification for the basic network information and important information systems related to the national economy and the people's livelihood according to the degree of importance and actual demand. The phased implementation and security information system can secure the normal operation of information and improve the comprehensive ability of information security protection, so that national security can be guaranteed, social stability and sustainability can be maintained, and the construction of information technology can be carried out in a benign way [7]. Therefore, China has conducted a unified management standard and technical standard for the hierarchical protection of network information, and has implemented an effective hierarchical protection mechanism for the information system through the organization of citizens, legal persons and institutions [8]. According to the provisions of Guidelines for the Classification of Computer Information System Security Protection, the information security level can be divided into five levels, that is, the first level is the user's independent protection level, which is primarily the way of users to protect resources. The second level is the level of system audit protection, that is, the security protection mechanism of this level is to provide technical support for improving the ability of users to protect themselves, especially in the ability to access audits [9]. The third level is the security tag protection, that is, the mandatory access control for visitors and interviewee is increased on the basis of the second level protection capability, so as to access the permissions set through different tags. The fourth level is structural protection, which extends the protection of the previous three levels to all visitors and interviewee, which has a strong resistance to penetration [10]. The fifth level is access verification, that is, the arbitration of the visitor's ability to access is increased on the basis of the fourth level of protection, which has a strong resistance to penetration. Fig. 1 shows the computer network information level protection mechanism publicity map.

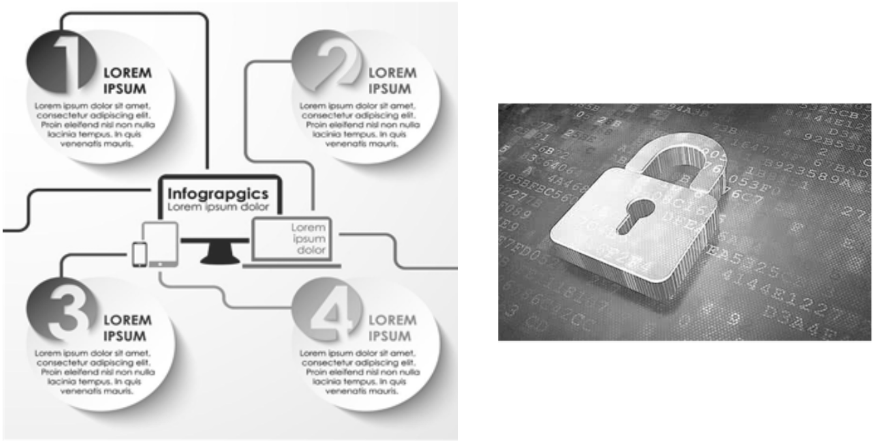
1
LOREM IPSUM
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin eleifend nisl non nulla lacinia tempus. In quis venenatis mauris.
2
LOREM IPSUM
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin eleifend nisl non nulla lacinia tempus. In quis venenatis mauris.
Infograpgics
Lorem ipsum dolor
Lorem ipsum dolor
3
LOREM IPSUM
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin eleifend nisl non nulla lacinia tempus. In quis venenatis mauris.
4
LOREM IPSUM
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin eleifend nisl non nulla lacinia tempus. In quis venenatis mauris.

Fig. 1. Propaganda diagram of the computer network information level protection mechanism

In the process of building the network information level protection mechanism based on the computer security model algorithm terminal, for the terminal security evaluation, it is necessary to classify the information security according to the test results in each structure, so as to realize the safe use of different security level requirements [11]. Therefore, the author chooses the support vector machine classification algorithm to construct the terminal security classification model. The ultimate goal is to realize the objective and accurate classification of terminal security level information. According to the literature, it is known that the support vector machine belongs to a two-class algorithm, which is obtained by super-plane acquisition through a high-dimensional space, and the sample is divided into two categories by the minimum error probability [12]. Support vector machine has the characteristics of global optimization, simple structure and easy popularization in the construction of terminal security classification model, especially it has obvious advantages in solving small samples, nonlinear recognition and high dimensional pattern recognition [13]. The model construction of the support vector machine architecture is carried out: firstly, sample data set training is carried out in a space of a given feature, that is, $T = \{(x_1, y_1), (x_2, y_2), ..., (x_N, y_N)\}$, $x_i \in \chi = R^n$ in the formula and $y_i \in \gamma = \{+1, -1\}, i = 1, 2, 3, ..., N$. Then, the model is constructed and the constrained optimization problem is solved, as shown in equation (1):

$$\begin{array}{l} \min\limits_{\alpha} \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_i \alpha_j y_i y_j (x_i \times x_j) - \sum_{i=1}^{N} \alpha_i, \\ \text{s.t. } \sum_{i=1}^{N} \alpha_i y_i = 0, \\ \alpha_i \geq 0, \ i = 1, 2, ..., N. \end{array} \tag{1}$$

By combining the theorem with the optimal solution $\alpha^* = (\alpha_1, \alpha_2, ..., \alpha_N)$in equation (1), the calculation is carried out, and the results are shown in formula (2) and formula (3):

$$w^* = \sum_{i=1}^{N} \alpha_i^* y_i x_i \,, \tag{2}$$

$$b^* = y_i - \sum_{i=1}^{N} \alpha_i^* y_i (x_i \cdot x_j) \ . \tag{3}$$

In combination with the above results, the hyperplane needed by the model can be obtained, as shown in equation (4):

$$w^* \cdot x + b^* = 0 \,. \tag{4}$$

So, the decision function can be drawn as shown in equation (5):

$$f^* (x) = sign (w^* \cdot x + b^*) \ . \tag{5}$$

According to the characteristics of the support vector machine, the author divides the security of the network information level of the computer terminal into four levels. So the model of this part chooses the hierarchical model to construct the classification. In the model structure, the decision function in the ith layer structure is expressed as $f^{(i)} (x)$, and when $f^{(i)} (x) = 1$, the $y = i$ sample points can be separated. When $f^{(i)} (x) = -1$, it will enter the next level of the decision. Figure 2 shows the module's hierarchical structure.

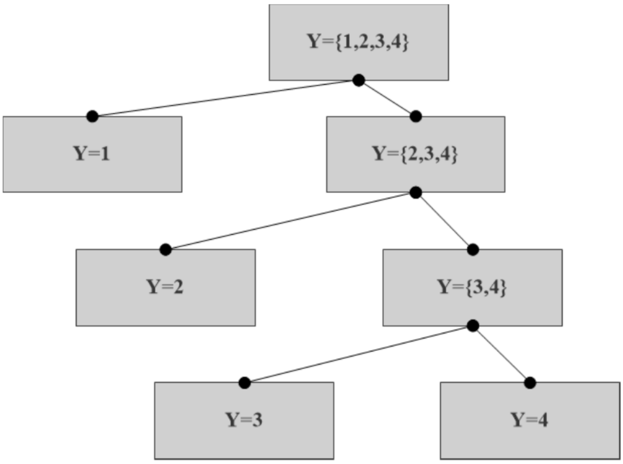

Fig. 2. Hierarchical diagram

As can be seen from the hierarchical structure diagram, in the first layer, the sample is divided into 1 class, and the division of the grade 2, 3, 4 is performed, so the new sample set is

$$T^{(1)} = \left\{ \left(M_1, y_1^{(1)} \right), \left(M_2, y_2^{(1)} \right), ..., \left(M_N, y_N^{(1)} \right) \right\},$$

$$T^{(2)} = \left\{ \left(M_1, y_1^{(2)} \right), \left(M_2, y_2^{(2)} \right), ..., \left(M_{N_1}, y_{N_1}^{(2)} \right) \right\},$$

$$T^{(3)} = \left\{ \left(M_1, y_1^{(3)} \right), \left(M_2, y_2^{(3)} \right), ..., \left(M_{N_1}, y_{N_2}^{(3)} \right) \right\}.$$

The following is the initial optimization problem, with the first layer as an example. In the sample set of the first layer

$$\begin{cases} y^{(1)} = 1, y = 1; \\ y^{(1)} = -1, y \in \{2, 3, 4\}; \end{cases}, i = 1, 2, ..., N.$$

The structural optimization problem is shown in equations (6) and (7):

$$\min_{\alpha} \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_i \alpha_j y_i y_j \left(x_i \bullet x_j \right) - \sum_{i=1}^{N} \alpha_i \, , \tag{6}$$

$$\text{s.t.} \sum_{i=1}^{N} \alpha_i y_i = 0, \alpha_i \geq 0, i = 1, 2, ..., N \, . \tag{7}$$

And then, the optimal solution is $\alpha^{(1)} = \left(\alpha_1^{(1)}, \alpha_2^{(1)}, ..., \alpha_N^{(1)} \right)^T$ and $w^{(1)} = \sum_{i=1}^{N} \alpha_i^{(1)} y_i x_i$ is calculated, and the positive component of $\alpha^{(1)}$ is chosen to calculate $b^{(1)} = y_j - \sum_{i=1}^{N} \alpha_i^{(1)} y_i (x_i \cdot x_j)$. Then, the decision function of the required hyperplane $w^{(1)} \cdot x + b^{(1)} = 0$ can be obtained, as shown in equation (8)

$$f^{(1)}(x) = \operatorname{sign}\left(w^{(1)} \cdot x + b^{(1)}\right). \tag{8}$$

So, when $f^{(1)}(M_i) = 1$, the network information security level is 1, when $f^{(1)}(M_i) = -1$, the network information security levels are 2, 3, 4, which then enter the next level of the decision. After entering the second and third layers, the decision functions are obtained by the above methods, as shown in equations (9) and (10):

$$f^{(2)}(x) = \operatorname{sign}\left(w^{(2)} \cdot x + b^{(2)}\right), \tag{9}$$

$$f^{(3)}(x) = \operatorname{sign}\left(w^{(3)} \cdot x + b^{(3)}\right). \tag{10}$$

Then, the network security level is judged and divided into the sample set.

In the aspect of the implementation of computer security model terminal network information level protection mechanism, the author believes that the implementation of module multilevel security mechanism mainly involves the following three aspects: the first is the access control decision module, which mainly marks the subject and object information and checks the information security strategy, accesses the request information of the resource access and the related security policies according to the subject and object, so as to provide corresponding ruling results for access control enforcement [14]. The second is the access control execution module, that is, according to the decision result of the upper module, it performs or rejects the access to the subject and object. In addition, the implementation of identity authentication module is needed. The authentication module mainly validates the users who use the information through the trusted hardware device to obtain the information authentication whose identity and user rights are consistent. At the same time, during the verification process, the system will perform mandatory access control, the provider's markup, and permissions [15]. The third is the security agent module, which mainly communicates with each other through the need of Windows node system and the security management control center, including the subject and object marking synchronization information, security policy download, audit information submission and other information. Table 1 shows the function index of Windows node subsystem.

3. Result analysis and discussion

This paper studied the implementation of the network information level protection mechanism based on the computer security model algorithm terminal. According to the above, the network information level security model was constructed. The model of the network information level protection mechanism was tested. Therefore, according to the principle of network information level protection, the model in this test first controlled the user's access behavior in the network communication on the basis of the rule. Among them, the subject in the system was the user, the object was the keyword. For subject of different levels, there was a difference in the right to use the object, so subjects with lower security levels had more restrictions on network communications than subjects with higher security levels. Thus, subjects with different levels of security could only use objects that were consistent with their security levels. If the subject had unauthorized use of the process of using the network information, the system would handle violations according to relevant regulations. The author divided the objects into five levels in the system, which were open, secret, confidential, top secret and prohibited. The security intensity of the five grades was: public <secret <confidential <top secret <prohibited. Therefore, the security level for the main body was divided into four levels, namely, open, secret, confidential and top secret. Table 2 shows the control authority of the subject access object.

Table 1. Function index of Windows node subsystem

Index type	Index content
Mark	It provides two-dimensional markings to mark the confidentiality level, integrity level, and security class of the entities in the system. The tagged objects include users in the system, all files and processes, ensuring that the tagged information is accurate, complete, and consistent throughout the lifecycle.
Forced access control	The mandatory access control mechanism implements the same security policy as the system two-dimensional security model, which can control all the operations of the process on the file. The mandatory access control mechanism should have some flexibility to combine the application process to check the behavior of processes that do not conform to the system's mandatory access control policies. This ensures that those that meet business needs without compromising system security can be enforced; mandatory access control mechanisms are always valid and will not be bypassed.
Identification	It can provide a secure identity authentication mechanism based on trusted hardware devices to ensure that unauthorized users cannot access system information.

Table 2. Subject access object control authority

Subject/object	Public	Secret	Confidential	Top secret	Prohibit
Public	allow	prevent	prevent	prevent	prevent
Secret	allow	allow	prevent	prevent	prevent
Confidential	allow	allow	allow	prevent	prevent
Top secret	allow	allow	allow	allow	prevent

In the case of the classification of the sample set, the security level of the sample set also needed to be divided according to the above-mentioned subject authority, in which the network information of the public level could be divided when the sample set was divided. Therefore, this experiment mainly divided four levels of secret, confidential, top secret and forbidden; secret was level 1, confidential was level 2, top secret was level 3, forbidden was level 4. Therefore, the three threshold values were set to the positive number, that was, η_1, η_2, η_3 and $\eta_1 = 25$, $\eta_2 = 50$, $\eta_3 = 75$. According to the three thresholds set, the four diversity points of the terminal were divided, symbol y representing the level and $y \in \{1, 2, 34\}$, then the available expression of y was:

$$\begin{cases} y = 1, \ 0 \le Y \le Y_1, \\ y = 2, \ Y_1 \le Y \le Y_2, \\ y = 3, \ Y_2 \le Y \le Y_3, \\ y = 4, \ Y_3 \le Y \le 100. \end{cases}$$

Here, the numbers 1, 2, 3 and 4 are the corresponding levels; the higher the security level was, the higher the security was. In this paper, by testing N computer network terminals 1 time, the resulting test results could be expressed with $M_1, M_2, ..., M_N$, and each test project was composed of various types of test items, there were all out of 100 points; the higher the score was, the better the security was, which could be expressed by $M_i = [m_1, m_2, ..., m_N]^{\mathrm{T}}$, $0 \le m_i \le 100$. At the same time, the total score for each calculation was expressed as $\overrightarrow{Y} = \overrightarrow{M_i^{\mathrm{T}}} \cdot \overrightarrow{H}$. Therefore, according to the above experimental process, the network information terminal of 55 known results was tested on the network information security protection mechanism. The test results are shown in Table 3. From the data in the table, it can be seen that the computer security model algorithm constructed in this paper can differentiate the hierarchical protection of network information. The result of the differentiation is consistent with the actual situation. Therefore, it can be proved that the network information level protection mechanism based on the computer security model algorithm terminal can effectively divide and classify network information and protect it effectively.

Table 3. Test results of network information security mechanism of network information terminal

Subject/object	Public	Secret	Confidential	Top secret	Prohibit
Public	5	7	2	3	1
Secret	6	9	3	0	2
Confidential	1	3	5	1	0
Top secret	0	1	1	3	2

As shown in Fig. 3, the statistical results of the effectiveness of the hierarchical protection mechanism for 55 network information terminals were presented. It can be seen from the figure that the network information level protection mechanism based on the computer security model algorithm terminal can achieve almost 100 % protection requirements, especially for information protection with high security level. But for the information protection mechanism with slightly lower security level, its efficiency is weak, which needs further improvement and analysis.

In conclusion, the network information level protection mechanism based on the computer security model algorithm terminal can effectively classify the computer

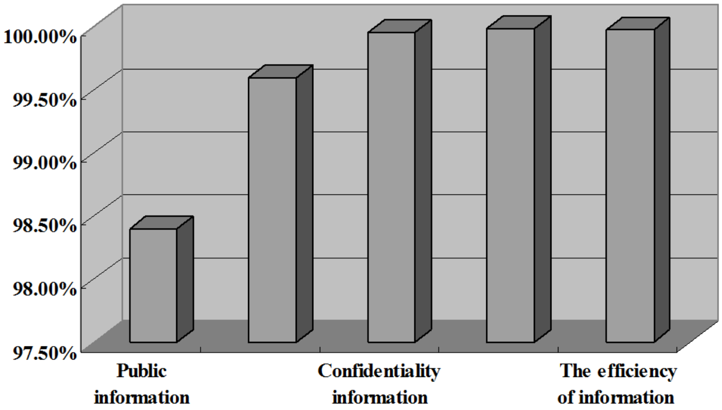

Fig. 3. Statistical results of the effectiveness of the hierarchical protection mechanisms for 55 network information terminals

network terminal information and protect it according to the security level of the network information. At the same time, the protection mechanism also divides users into different grades and uses different request limits for network users in different grades, so as to protect different levels of network information. And the experimental results show that the network information level protection mechanism based on the computer security model algorithm terminal is effective in network information protection. However, the protection of network information with low security level needs to be improved.

4. Conclusion

Network information plays an important role in people's life and work, and people depend more and more on it. At the same time, the increasing of network information also makes its security problems increasingly prominent. How to improve the security of network information has become the focus of the computer security model. In this paper, through the construction of computer security model, the network information security level division model was constructed according to the actual situation, and the user's level and the security level of the network information were divided. Through the computer terminal test, it can be found that the computer security model constructed in this paper can effectively divide the network information, and optimize the structure of the model to improve the efficiency of information classification. In addition, the user's level division can effectively protect the network information, users of different grades open corresponding network information, thus reducing the request rate of network information with high security level, thereby improving the protection of network information. However, it can be seen from the test results that the protection of low-security network information is not in place, in certain probability, network information cannot be protected, which needs further improvement.

References

[1] S. Kajioka, N. Wakamiya, H. Satoh: *Implementation and evaluation of multichannel multi-interface routing mechanism with QoS-consideration for ad-hoc networks.* EURASIP Journal on Wireless Communications and Networking (2010), Article ID No. 4074927, 1–14.

[2] K. Gopalakrishnan, R. V. Uthariaraj: *Acknowledgment based reputation mechanism to mitigate the node misbehavior in mobile ad hoc networks.* Journal of Computer Science *27* (2011), No. 8, 1157–1166.

[3] M. Ahn, J. Kwon: *Design and implementation of ontology-enabled context-aware platform in ubiquitous environment.* Angewandte Makromolekulare Chemie *86* (2006), No. 1, 203–213.

[4] T. E. Carroll, D. Grosu: *An incentive-based distributed mechanism for scheduling divisible loads in tree networks.* Journal of Parallel and Distributed Computing *72* (2012), No. 3, 389–401.

[5] D. V. Prieto, L. R. I. Quiñones, D. G. Ramírez, G. Z. Fuentes, P. T. Labrada, H. O. Pérez, V. M. Montero: *Impact of the information andc ommunication technologies in education and new paradigms in the educational approach.* Revista Cubana de Educación Médica Superior *25* (2011), No. 1, 95–102.

[6] L. Caviglione, M. Gaggero, J. F. Lalande, W. Mazurczyk, M. Urbański: *Seeing the unseen: Revealing mobile malware hidden communications via energy consumption and artificial intelligence.* IEEE Transactions on Information Forensics and Security *11* (2016), No. 4, 799–810.

[7] M. Alsaleh, P. C. van Oorschot: *Revisiting network scanning detection using sequential hypothesis testing.* Security and Communication Networks *5* (2012), No. 12, 1337–1350.

[8] P. Szwed, P. Skrzyński: *A new lightweight method for security risk assessment based on fuzzy cognitive maps.* International Journal of Applied Mathematics and Computer Science *24* (2014), No. 1, 213–225.

[9] P. Zand, S. Chatterjea, K. Das, P. Havinga: *Wireless industrial monitoring and control networks: The journey so far and the road ahead.* Journal of Sensor and Actuator Networks *1* (2012), No. 21, 123–152.

[10] Y. L. Chong, K. B. Ooi: *Collaborative commerce in supply chain management: A study of adoption status in Malaysian electrical and electronic industry.* Journal of Applied Sciences *8* (2008), No. 21, 3836–3844.

[11] M. S. Babu: *Operating systems-functions, protection and security mechanisms.* Resonance – Journal of Science Education *7* (2002), No. 4, 60–66.

[12] A. Nafarieh, S. Sivakumar, W. Robertson, W. Phillips: *SLA-based time-aware provisioning mechanisms in shared mesh protected optical networks.* The Computer Journal *58* (2015), No. 8, 1717–1731.

[13] Y. Jian, s. Chen, Z. Zhang, L. Zhang: *A novel scheme for protecting receiver's location privacy in wireless sensor networks.* IEEE Transactions on Wireless Communications *7* (2008), No. 10, 3769–3779.

[14] J. Sprague, D. Clements, T. Conlin, P. Edwards, K. Frazer, K. Schaper, E. Segerdell, P. Song, B. Sprunger, M. Westerfield: *The zebrafish information network (ZFIN): The zebrafish model organism database.* Nucleic Acids Research *31* (2003), No. 1, 241–243.

[15] Y. Jiang, J. Zhao: *An empirical research of the creative process of collaborative e-business capability in service industry.* International Journal of Networking and Virtual Organisations *10* (2012), No. 1, 73–870.

Received August 7, 2017