

2014

# BioTechnology

*An Indian Journal*

FULL PAPER

BTAIJ, 10(22), 2014 [13714-13719]

## Application of computer network security system in modern enterprises

Li Hua

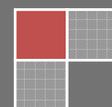
College of Computer Science and Technology, Taizhou University, Taizhou, 225300, (CHINA)

### ABSTRACT

With the rapid development of information technology, the corresponding computer technology has also been improved, and provides opportunities for the informatization construction of enterprises. But in the current situation, a series of security problem of the network of openness and sharing is becoming more and more serious, which gives the application of computer security system in modern enterprises higher requirements, and which is the key to the study. Internet is occupying the important status in the national information security strategy, the network security is a tight coupling of technology, system, tools and management, modern enterprises want to be in an impregnable position in the competition in the society, the construction of computer security system plays the irreplaceable role to ensure enterprise information storage, transmission, highly confidential data, and information advantage better participate in market competition so the study on it is in urgency. This study takes the generation of security problems of computer network security system and the main threats as the breakthrough point, to study the physical security management strategy, access control strategy, database security, etc., in order to guarantee the computer network information security in modern enterprises, and find out effective measures according to the relevant circumstances, thus to create conditions for the healthy and orderly development of computer network security system in modern enterprises, to better serve the study and life of people, and to provide strong theoretical support for the majority of researchers.

### KEYWORDS

Modern enterprises; Computer; Network security.



## INTRODUCTION

The construction of computer network system in modern enterprises breaks the original restriction of time and geography, making it possible of resource sharing; to some extent improve the enthusiasm of the staff, and to lay a solid foundation for enterprises to better participate in international competition. Computer network has the characteristics of wide distribution, open architecture, and resource sharing, etc, but influenced by various factors, in the process of transmission it could be illegal wiretapped, information intercepted, tampered, and even destroyed, resulting in serious losses<sup>[1]</sup>. Especially in terms of data security and confidentiality, if the computer information system of enterprises is damaged, it will directly affect the development strategy formulated previously by enterprise. Chinese computer network security system in modern enterprises has a large gap compared with western developed countries', particularly the modern enterprises not fully realize the importance of computer network security, and with the continuous production and propagation of computer viruses that some criminals use technical means for enterprise information to pursue illegitimate profits, which brings immeasurable loss to the national enterprises, therefore, it is urgent to study computer network security in modern enterprises.

## OVERVIEW OF COMPUTER NETWORK SECURITY

Computer network security is through the effective management of network, through monitoring, and the implementation of various technical means to ensure the network data's confidentiality, integrity, reliability, controllability and availability. The construction of computer network security system in modern enterprises is a relatively complex process, including the hardware network, software application, communication protocol and the operating system, covering the construction of multi-level security system<sup>[2]</sup>. After a long time's development, computer network security system has formed a complete set of model solution, which is composed of security service plane, protocol level plane, entity unit plane, safety management plane and other aspects, the construction of the model solution pointed out the direction for computer network security system in modern enterprises, help enterprises information for systematic and scientific overall, and creating a relatively stable environment development, to achieve the purpose of many aspects of network security system certification, which in some extent ensure the normal operation of the computer network system, and create conditions for the orderly development of network services. As the situation of Chinese enterprises participating in international competition narrowed, the modern enterprises have achieved office automation, production sharing, confidential business information, etc., but there are still many problems to solve. Throughout the current trend of enterprise development, the future commercial battle, information technology will be one of the key technologies, which also takes advantage of network core. Network can best meet the needs of the enterprise information, the future information warfare of enterprise is adapted to social development needs, and the construction of computer network security system in modern enterprise has developed a broader field for the enterprise to participate in international competition<sup>[3]</sup>.

## THE GENERATION OF THE SECURITY PROBLEMS OF COMPUTER NETWORK SECURITY SYSTEM AND THE MAJOR THREAT

### The generation of the security problems of computer network security system

The generation of security problems of computer network security system is mainly because of disturbance by many unsafe factors on information system to make the program disorder, on the other hand is due to the extreme importance of computer network security system and their own vulnerability. Before information system is simply in the form of computer, its security and privacy are determined by the user himself, basically not affected by external factors. But along with the rapid development of information technology, PC and mainframe system emerge as the times require, the corresponding server mode change, computer network has been linked closely with people's study, life, it can handle international confidential documents involving military, economy, politics and many other fields, and can also help the enterprise to deal with business information, and even personal privacy. Computer information network has become the information preservation and processing tools, which is the cause of the computer network security system in facing serious challenge<sup>[4]</sup>. On the basis of the current computer network security system, from the perspective of hardware, it belongs to the category of the binary logic device, and from the software side, it belongs to the category of tree table processing system, and the tree table is the main tool of current computer software application<sup>[5]</sup>. From the essential content, tree table can affect or reflect longitudinal relations and attributes, but can't do horizontal intrusion. In the process of computer software perfection, it will be influenced by many factors, so may be a potential safety hazard, which will create the possibility for other viruses' invasion. What's more, computer network security system itself is lack of relatively complete safety monitoring, there is a contradiction that cannot coordinate between local rational and the overall physical, combining with the characteristics of information opening, information resource sharing and so on, to make the computer information system serve for people's study and life, but at the same time, there are a lot of shortcomings, as is shown in Figure 1 the data processing algorithm flowchart of enterprises.

(1) Computer network security system used relatively sensitive commercial products. In the modern enterprises these commercial products are in a common computing environment, and its design original intention and purpose is to be competent of functional diversification and unpredictability of adapt to the environment, as well as investment can be profitable, not fully realize the importance of computer network system, which is also the important reason of the computer network security threat.

(2) Computer network security system involves range wide. "Computer network security system" in current has remarkable complexity and the boundary can not be clearly defined. Even for internal system, the information has many

uncertain factors and the threat to the system is from various fields and from anywhere, which will invisibly increase the difficulty for information security.

(3) The communication of internal modern enterprise is very frequent. The communication is not simple personnel communication, it is information communication and may also be the carrier exchange, and includes intangible electronic access, which can be simply divided into two aspects: first, access in conformity with legal benchmark; second, breaking the law for illegal access to obtain illegitimate profits, and thus lead to measures that rely on traditional position "isolation" to ensure information security is undesirable.

(4) Criminal activities under the inducement of profits. Some hackers use their advanced technology into the "vacuum" of computer network to steal and modify the data, so as to obtain illegitimate profits.

(5) Affected by "information right" under the new situation. The future commercial struggle should be built around information utilization and the anti-utilization, if enterprises take the information advantage, they will create conditions for market advantages.

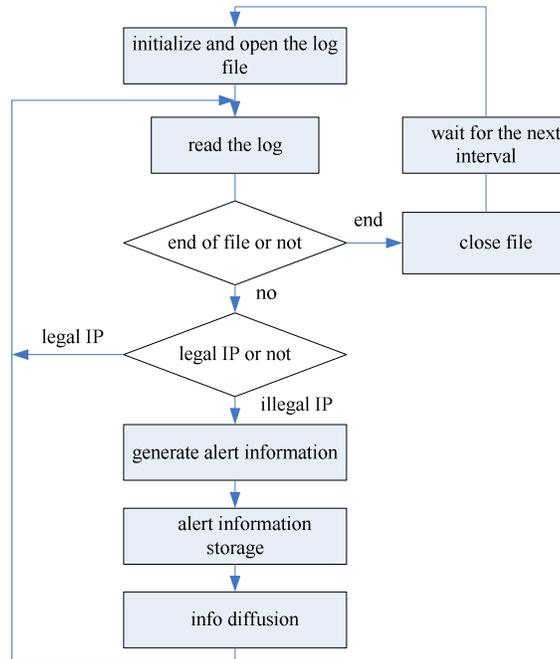
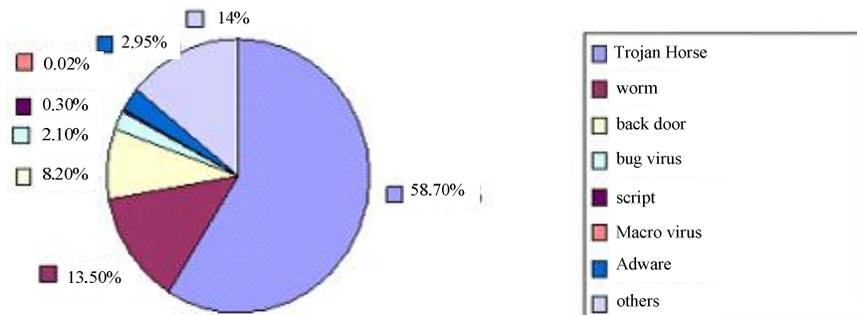


Figure 1 : Data processing algorithm flowchart of enterprise

**The main threat of computer network security system**

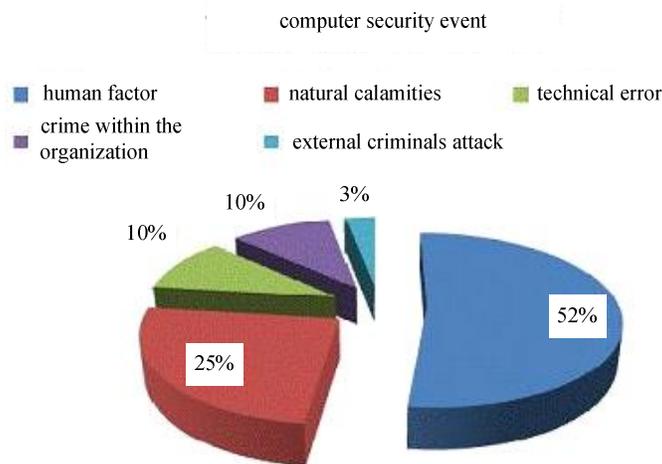
As is shown in figure 2: from common sense, the threat of computer network security refers to: integrity of information is damaged, confidentiality of information is lost or disclosure and information services are interrupted, etc. The US department of justice gave a clear definition to the threat of computer network security system: "Any events associated with the computer technology, a victim may suffer losses in the event, and abusers may have the intention to obtain or have obtained benefits. Except for correct business strategy, the modern enterprise shall also ensure that enterprise information does not exposure, which to a certain extent can prevent the occurrence of vicious competition. Because computer information has the characteristics of sharing and easy diffusivity, etc, there is a great risk in processing, storage, transmission and usage, and easily distracted by other factors to cause data loss or misuse, and may also be affected by other viruses, in particular, the current computer network security system is facing the influence from the users or other factors. Mainly displays in: unauthorized access, information disclosure, system function damage, computer virus, jamming system services, etc.



**Figure 2 : Threat generated by various types of virus**  
**SECURITY MANAGEMENT STRATEGY OF COMPUTER NETWORK SECURITY SYSTEM IN MODERN ENTERPRISES**

**Physical security management strategy**

As is shown in figure 3, the attack of computer network security system is mostly by external illegal personnel, the smallest percentage is human factors. The original intention and purpose of physical security management strategy is to protect the computer system, network server, printers and other hardware from other factors; In using process it can effectively test and verify the identity and permission of the users to ensure that information is not leaked; to establish and improve the computer network security system management and to prevent criminals from entering the computer to steal information to obtain illegitimate profits.



**Figure 3 : Architecture diagrams of computer events**

**Access control policy**

Access control policy is the main policy for security protection of computer network security system and for self-protection in modern enterprise, its task is to ensure that the enterprise information from illegal access, which must be in normal operation procedure to obtain. At the same time it is also the important means to maintain data security of computer network security system in modern enterprise, a variety of security measures must complement each other and work together to fully reveal the real protection function, an access control policy occupies the core status in all policies. Figure 4 is the various factors of enterprise network virus invasion. To solve these problems need to take the necessary strategy to control:

(1) Network access control. Network access control provides the first layer access control for network access. In modern enterprises, information sharing can improve work enthusiasm of staff and create conditions for employees' better communication, network access control is the same as it, it is able to control which users have a login permissions and whether to have qualification to acquire network resources. Network access control can be simply summarized as three parts: login user permissions, user information identification and user information check. If there is one program error in above procedure, the user does not have the permission to login to make it impossible to obtain network information. User login permission is the key for users to access network and acquire resources, so in the process of building computer network security system, a modern enterprise should carry out encryption for a user's password. The common encryption methods are password encryption of one-way function, encryption password based on test mode, password encryption based on quadratic residue, etc. In this process, the network manager of the enterprise should limit the use of ordinary account, the manager should also audit to the customer, if multiple input account or password are wrong, it will be locked, if illegal access to a specific value, the server will alarm in specified way, which is also the important measures to ensure that information is not illegal used.

(2) Firewall control. Firewall control is a technical measure of computer network security gradually developed and formed in recent practice, its application to computer network security system in modern enterprise in some extent prevent hackers from accessing to an organization, in another word, it can be called a threshold that control into/out in two directions, to ensure that the network boundary set up corresponding network monitoring, to make internal network and external network both can be effectively separated, to offer the possibility to block external network intrusion, to create conditions to ensure information safe and reliable of the enterprise. The current firewalls are mainly: packet filtering firewall, dual-homed host firewall, and screened host gateway firewall, etc<sup>[6]</sup>.

(3) Smart card technology. Smart card technology is done on the basis of digital encryption technology; it is also the alternative name of secret key. Take the credit card as an example, which is also specific to authorized users, who just enter specific instructions or relevant information, as only as the information matches the server's password it is able to go to the

next phase of operation. The application of smart card technology for construction of computer network security system in the modern enterprise for confidential business information is quite effective.

(4) VPN technology. The core of VPN technology is the tunneling technology, which is that the data input to a specific channel for transmission, so as to get their needed information. VPN system is a relatively systematic and scientific solution, including many other computer technology: a number of mechanisms, identity, login authentication, encryption and secret key distribution<sup>[7]</sup>. A safe VPN used security protocol for data transmission in tunnel or specified tunnel, which has a high confidentiality and reliability, these protocols can negotiate to use digital signature technology between hosts, to ensure the confidentiality of enterprise information, prevent from others stealing, and data can be complete and will not be interfered. In the concrete implementation of VPN technology in enterprise, pure software platform, specified software platform and other software platform can be used.

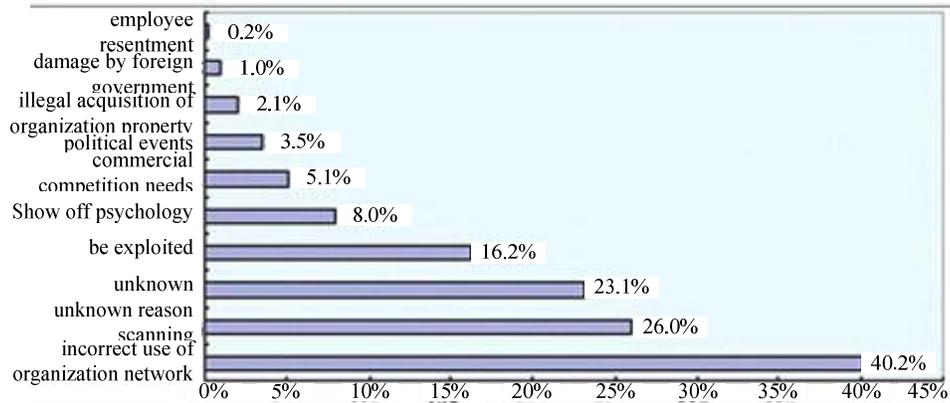
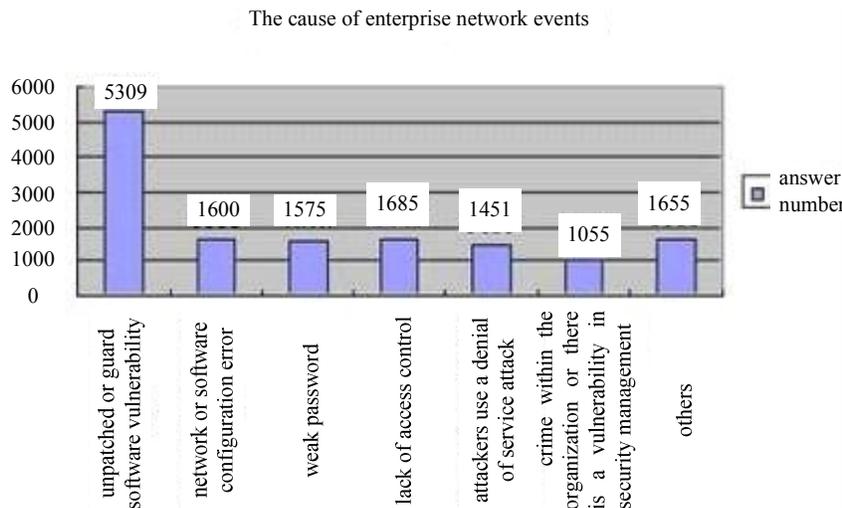


Figure 4 : Various factors of enterprise network virus invasion

Database security

As is shown in Figure 5, the biggest factor of enterprise network virus invasion is unpatched or guard software vulnerability database technology, the smallest factor is crime within the organization. Database technology can be trace back to the 1960s, after a long time of development it has now become one of the key technology of computer technology. From the essential content, it is a branch of software subject, database technology and network communication technology, a specific object-oriented technology become the main characteristics of the current computer technology development<sup>[8]</sup>. Database is the geometry of the related data, which contains the data of not itself, but the associated data. Database technology is devoted to the research of data access, use, and systematic management. With the further development of computer network security system, it can be implemented resource sharing of computer hardware and software on the basis of the original level. Network database is based on computer network environment, at the same time can be used by multiple databases, and ensure that the data is not lost, not steal by others. Computer network is a main application and can achieve data information sharing by network. Resources in network database are not restricted by time and place, as long as the users need it is able to login specific database to download or browse the information they need<sup>[9]</sup>. In particular, the database security is under the management and control of the database management system (DBMS), and DBMS is completed based on the operation, which also includes data resources, which will not allow users to ignore the DBMS to directly operate system to get the data, it must be in accordance with the relevant procedures, to a certain extent to ensure the enterprise information safety, and lay a solid foundation for better participating in the competition.



**Figure 5 : The cause of enterprise network events**  
**CONCLUSION**

The rapid development of economy put forward the deeper challenge for computer network security system in modern enterprise, so it requires the modern enterprises that according to their situation to build computer network security system to ensure the high confidentiality of enterprise development strategy. This paper studies the generation of security problems of computer network security system and the main threat, and on this basis to find the security management strategy of computer network security system in modern enterprise, to ensure the safe reliability of information, reduce the interference by other external factors, create a favorable environment for healthy development of the enterprise, and better participate in market competition.

**REFERENCES**

- [1] Yin Shenming; Security policy of e-government information system [J], *Computer Era*, **8(4)**, 31-34 (2006).
- [2] Fan Xiaolei, Qi Xiaoguang, Wu Di; Research on the computer network security and precautions [J], *Science and Technology of West China*, **8(16)**, 22-23 (2009).
- [3] Ye Xiaoming; Talk about network security [J], *Economic Window*, **7**, 12-13 (2010).
- [4] Cheng Yikang; System and development of modern network security [J], *PC World*, **6**, 23-25 (2013).
- [5] Wu Qian; Discussion on constructing technique of e-government extranet metropolitan area network [J], *Network & Computer Security*, **9(7)**, 41-44 (2012).
- [6] Huang Zongjiang; Analysis and prevention of e-government network security [J], *Computer & Network*, **18(4)**, 53-56 (2006).
- [7] Deng Yameng; Safety construction of enterprise office network [J], *Modern Computer*, (9), 42-44 (2005).
- [8] Zhao Ge, Qian Depei, Fan Hui; Construct network security system with distributed firewall [J], *Application Research of Computers*, (2), 45-47 (2011).
- [9] Fan Xiaolei, Qi Xiaoguang, Wu Di; Research on the computer network security and precautions [J], *Science and Technology of West China*, **8(16)**, 22-23 (2009).