IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 4, April 2017

Research on Security Issues and Protection Strategy of Computer Network

Gurdeep Singh[1], Gurjeet Singh[2], Gurwinder Singh[3], Er. Charanjit Kaur Raina[4]

CSE Department, Adesh Institute of Technology, Gharuan, Punjab, India[1,2,3]

HOD, CSE Department, Adesh Institute of Technology, Gharuan, Punjab, India[4]

Abstract: Development and improvement has brought a very great impact to the network technology of the computer, besides the security of the network information has become a focus of the social safety questions. In this paper, through the analysis of security threats to computer network information and protective factors conducted, a strategy for a common computer network information security and protection strategy has been proposed, and useful lessons for our computer network and information security and protection reference have been provided. A series of questions such as security and dependability regarding the computer network system arise, which has been taken into consideration in proposing the strategy. This paper puts forward proposals with respects to the importance of the computer network system, existing problems of the online security of the computer, and precautionary measures. The detailed discussion will help the mass users to become conscious regarding network security and take precautionary measures while using the network.

Keywords: Computer Network, Network Security, Preventive Measures, Security protection system.

1. INTRODUCTION

In essence, network security means information security on the network, which requires that the flow of network systems and data saved are not subject to accidental or malicious destruction, disclosure or alteration. Therefore, the data in transit is vulnerable to attack. On the entire data communication networks, data protection measures must be taken to include including the legitimacy of the data confirmed and the legitimacy of the communication data ensured. In a net- work running, large amount of data and information are stored in the host or terminal that is the external memory, so how to prevent unauthorized users access is essential to ad- dress network security issues.

In the actual computer network, security management will often face attacks, such as unauthorized use of the IP address phenomenon, which not only affects the normal use of the computer network, but also due to unauthorized use of address tends to have a higher authority. The enterprise unit caused a lot of economic losses and potential safety hazards, hence anti-attack has become an important research field of computer network security. Core attacks refers to sending fake response to the target host, and the target host receives the forged response mapping between IP and MAC, and thus updates the target host cache. People enjoy the great benefits of the Internet, while the challenge of the convenient net- work security is unprecedented. Network security needs to be 100% secure. If the system is damaged, the data is lost, and confidential formation may be stolen imparting direct and indirect economic losses. Hacker attacks the network and such intrusions caused a great threat for national security, economy, and social life. Currently, information on how to Protect the system’s inviolability and how to effectively prevent the unlawful invasion and how to address security issues to protect a series of information, has developed into a sizable industry.

2. COMPUTER NETWORK SECURITY ANALYSIS

Using Physical Security Network is the premise of the entire network system security. Physical security is defined as the physical medium level of network storage and transmission of information’s security protection is essential to protect the network information. To establish physical security architecture, three aspects should be considered: First, natural disasters (earthquakes, fires, floods), physical damage (hard disk is damaged, aging equipment, external damage) and equipment failure (power, electromagnetic interference); second includes electromagnetic radiation, taking advantage of infiltration, traces of leakage; and third includes operational errors (hard disk formatting, line removal), accidental omission and so on. Computer network application technology, the Internet is representative of the network, which now has developed into a global information network to share and become a part of people's lives. Network not only changed people's production, living and learning environment, but also affected people's way of thinking.

Now the Internet has become an indispensable part of our lives, since it has fully infiltrated into the commercial, financial, government, health care, research, education, and other social sectors. Whether it is Internet, LAN, or even

DOI10.17148/IJARCCE.2017.64160

GPRS cellular communications, the power of the network is always reflected in the daily life. With the development of the Internet, the number of new industries boasted, such as online games, online chat, on-line video download, besides network media, e-commerce, e-government and other companies, to bring more business opportunities. Network topology design also has a direct impact on the security of the network system. If there are both external and internal communication networks, the machine is not only likely to receive internal network security threats, but also affect other systems on the same network and other networks connected to the Internet / Intranet. Therefore, we need not only to adopt a server at the time of design (WEB, DNS, EM AIL, etc.), which could better provide better security and necessary isolation from other external and internal business networks, avoiding net- work structure information leakage; but also a service re- quest to the external network filter, allowing only normal communication packets reach the appropriate host, the other request service before reaching the host should be rejected.
Security system refers to the entire network operating system where the network hardware platform is reliable and trustworthy. There is no absolute secure operating system available that can be selected. Regardless of operating system, the development company must have its reserve entrance for troubleshooting and a detailed analysis of their network should be conducted with respect to different user’s different aspects. Besides, the highest possible safety and operating systems hardware platform, operating system and security configuration should be chosen. It also needs to strengthen certification (especially certified before reaching the server host) login process to ensure the user's legitimacy. Next, there should be strictly limited operating authority registrant, which can control the minimum range of the operational limits

3. COMPUTER NETWORK SECURITY PROBLEMS

With the advent of the Internet age, people have been enjoying the endless joy the network has brought. On the other hand, they are also facing an increasingly serious and complex network security rib, and the risk aversion is difficult. The original damage caused by single computer security incidents may spread to other systems and the host, causing extensive system paralysis and loss. Due to the lack of security control mechanisms and the lack of network security policies and protection, awareness of these risks is increasing (Fig. **1**). Through the analysis of computer network information security threats and protective factors conducted and presented as a basis for a common computer network information security and protection strategy, we look forward to provide useful lessons for our computer network and information security and protection reference.

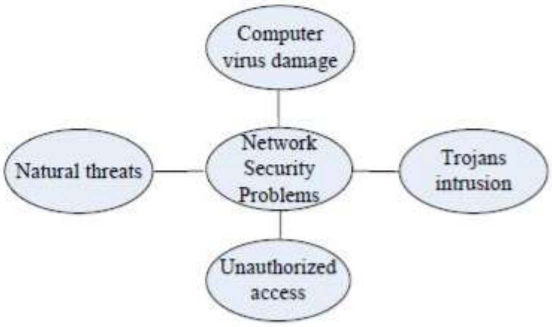

Fig. (1). Computer network security problems.

Natural threats may come from various natural disasters, poor site environment, electromagnetic radiation and interference, network equipment and other natural aging. These activities are no purpose in sometimes, they will threat the security of the network directly or indirectly, and they will influence the storage and exchange. As the invasion began, hackers had developed a “reserve entrance” technology, through the use of this technology, one can enter the system again. Backdoor functions are in the following sequence: making the administrator to stop the growers enters into the system again so that growers can’t be easily found in the system; the system allows growers minimum time spent to enter the Trojan, which is also known as Trojan horses. It is a special kind of English word called "Trojan horse", whose name is taken from the Greek myth "Trojan horse in mind”. It is a hacking tool based on remote control, covert and unauthorized characteristics. In general, there are two Trojans programs, one is a server program and the other is the controller program. A Trojan server program is required if the controller program is installed in a computer. The hacker can use Trojan controller program into this computer, through the command server program to control PC port.
Unauthorized access refers to writing and debugging skills have been installed in computer programs that are being used to get the network access or file law between legal and illegal or grant access to the other party for intrusion to the intranet. Network intrusion prevention system is mainly made for permission storage to use the system, write permissions and provide access to other stored content, or as a springboard for further access into other systems, or

DOI10.17148/IJARCCE.2017.64160

malicious damage to the system that it destroyed and lost service capabilities. Referring to the preparation of a computer virus in a computer program or destruction of computer functionality data inserting, computer instructions or self-replicating code could be used with network intrusion prevention sys- tem. Such as the common worms, they regard the computer as a carrier, which exploits the operating system and the application of the initiative to attack. It is thus a vicious virus passing through traditional network. There are some com- mon viruses, such as the spread of 'covert win' in traditional network, which is not only destructive and latent, etc., but also has some of its own characteristics, such as not using an arbitrary existing file as parasitic host (some only exist in memory), resulting in a denial of service on the network, as well as the combination of hacking techniques and so on. Other common destructive viruses have relatively strong macro viruses, for example Italian sausages.

4. REQUIREMENTS ANALYSIS OF NETWORK SE-CURITY

The defensive system is capable of rapid deployment, without changing the existing network topology. Using such access devices, you can continue to open networks. We need to install client software, which can solve the virus attack problem and collect multiple network segments, through a plurality of the communication program, in physical space permitting, to collect multiple routers under communication. We can adapt to a variety of network environments, such as manually assigned IP, automatic Indian song allocation of IP etc., as well as can adapt to the frequent changes in the net- work and IP hosts. It is easy to operate even by non- professionals after a simple training immediately after the operation. The research found that many enterprise network managers are non-professional, and the situation particularly gets even more serious in the various colleges and universities. In the case of Pinpoint attack packets, one can distinguish between normal communication and attack.

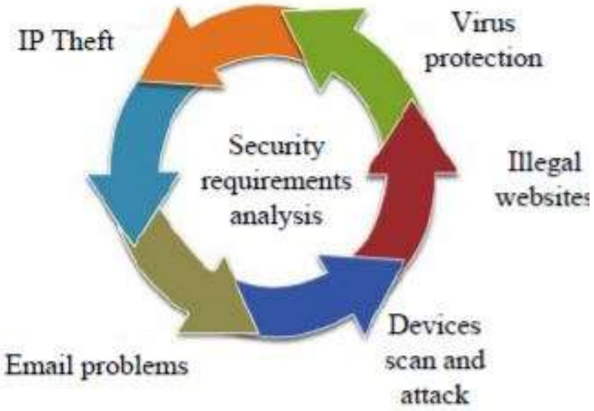

Fig. (**2**) shows the requirements analysis of network security.

In the case of Intercept attack, the system's kernel level is made to intercept external fake packets to protect the system against spoofing; such attacks effect maintains smooth net- work and communications security by monitoring cache. If automatic monitoring of the local cache table is found to be tampering with the MAC address changed due to the gateway malicious programs, network antivirus provides necessary complement to respond to the overall solution. However, the system is only found responsible for blocking the attack, but does not involve the work of clearing the virus. We should take initiative to maintain communication with the gateway, so that the gateway advertises the correct MAC address. In order to maintain smooth network and communications security, the attacker has to be traced. According to the packets in the data to lock the attacker IP address, a virus has been designed to kill. Virus signatures have been used to scan the system for viruses, providing protection from the cache. The system also prevents from malicious tampering with the local cache program.

5. THE OVERALL DESIGN OF DEFENSIVE SYSTEM

With the evolving means of attack, relying on traditional firewalls, encryption and authentication and other means for system's protection, has failed to meet the requirements. In the modern network security system, monitoring and response are gradually becoming increasingly important, in building the network security system as an important part. This is not just a simple process of running protection net- work, but also includes network security assessments and the use of security technology after service system. With the rise in dependency on the network, and emergence of hacking tools, the traditional network information security is so far failed to meet people's requirements for information security, due to which the construction of network information security system has been welcomed by all. Construction of the network information security system based on the original network not only includes additional protection network security assessments, but is also programmed to use of network protection technology after service system and achieve comprehensive, multi-technology to maintain and protect computer information security.

From the above, we can find that prevention from the principle attacks, that is spoofing attacks, is not the biggest difficulty that lies against the server or switch of the system itself, but also the source attack segment that can be hidden in any of the places in the system, which means its hidden high prevention and treatment of common attacks and viruses as a single or as the preventive effect from the network gateway of the server system is not very good. Therefore, we proposed an attack prevention strategy that needs to simultaneously start three-pronged steps: Computer system security reinforcement, MAC-mapping table management, and net- work illegal packet detection.

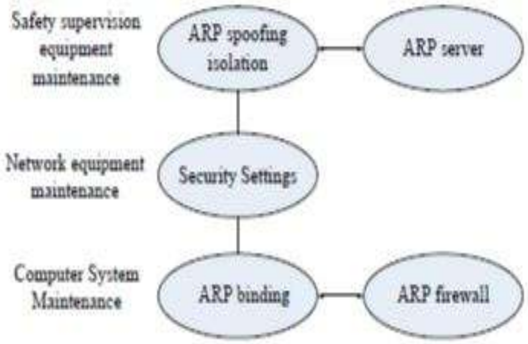
Safety supervision equipment maintenance
ARP spoofing isolation
ARP server
Network equipment maintenance
Security Settings
Computer System Maintenance
ARP binding
ARP firewall

Fig. (3). The framework of attack defend system.

System network port is connected to the switch mirror port to charge all packets; the system network interface has to be in the promiscuous mode, in order to meet the needs of multiple segments that can be collected. Information system can be set to receive each data. System hardware platforms need to install multiple Ethernet ports for connecting the switch to multiple routers. Fixed system is used to convert all dynamic static, thus effectively preventing the attacker to modify the entries. This method is relatively simple, since as long as the device type is in fixed command, the device will be the fixed system that converts all dynamic static.

Specific methods of various means of comprehensive protection system are: setting a static MAC to IP mapping table, and prevent hackers from refreshing static conversion table. The network security relationship should not be established on the basis of the IP or MAC, instead the trust relationship should be established based on the IP + MAC. Use MAC address management server. Find your own translation table by the server to respond to broadcast or to other machines. Isolate entrusted domains using a firewall internal network machines packet transmission. Use detection tools to detect illegal broadcast data frames on the network.

6. NETWORK AUTHENTICATION TECHNOLOGY

Along with rapid development of the computer and the Internet technology, many enterprises are gradually realizing the computerized management of business, and have accumulated a large amount of historical business data. The data volume is growing rapidly. More and more enterprises are using data warehouse technology to summarize process and analyze data. Extract, transform and load (ETL) process is the key link for building data warehouse. If the ETL can help users neatly implement the ETL solution, the data warehouse IP Theft Email Problems Devices scan and attack Virus Protection Illegal Websites Security requirements analysis

Fig. (2). Requirements analysis of network security. solution can also be implemented smoothly. And the ETL processing efficiency directly affects the data loading efficiency

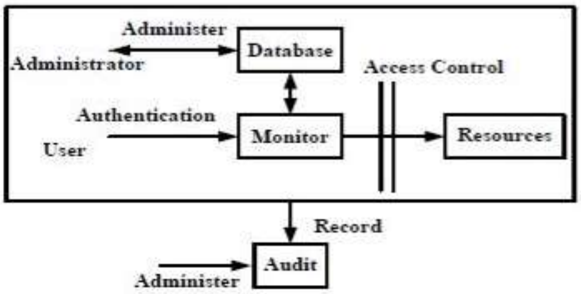

Fig. (4). The Logical structure of the safety system.

DOI10.17148/IJARCCE.2017.64160

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 4, April 2017

In the distributed data warehouse, every local data ware- house is a self-governed ETL node. Because of the existing data copies, the distributed ETL has multi-targets. If the traditional ETL architecture is still used in the distributed data warehouse, there will be inconsistent data present in the local data warehouse as a result of central ETL architecture. After analyzing the deficiency of central ETL architecture, an improved advanced distributed ETL architecture-ETLM has been proposed to resolve the problem of data consistency in the distributed ETL in a better way.

The distributed data warehouse has many local ETL nodes; every node will process plenty of data. After being transformed, the data needs to be loaded on multi-local data warehouses. In this situation, the traditional technology of data extracting and transforming may not be effectively helpful since it has many deficiencies, especially on response time and transform efficiency. According to the demand of OLAP and DM, a new optimized method for executing distributed ETL has been put forward. The method is based on the strategy to combine data segmentation and load balancing technologies. ETL technology and distribution technology are both used in executing this strategy. The strategy is intended to make up the disadvantage of low efficiency when executing distributed ETL. The globe efficiency of distributed data warehouse will be improved after applying the strategy

7. THE DESIGN PRINCIPLES OF AUTHENTICA-TION SERVER

With the expansion of the enterprises on both large and small scale, the operations in the enterprise spread too many regions. And the operational pattern of many enterprises forms a kind of distributed management structure. Besides, as a result of changing history, geography, and economy and so on, there are many transaction processing systems which are self-governed and do not have compatibility with the enterprises, so we need to integrate these data, which are distributed in these systems, with the systems in order to offer uniform data views to the decision-makers. That's how distributed data warehouse came into being. The process of data using ETL is important in establishing data warehouse especially for caching. Therefore, the ETL technology has always been a hotspot in the research of distributed data warehouse. Fig. (**5**) shows the network structure of authentication server.

The strategy sequence of ELT, Data extract, data trans- form and data load, is as follows; Using configurable files define and display the business logic; provide the simple interface for helping users understanding and using the ETL system. Use the connection pool and JDBC technology at the data extract and data load process to enhance the database connection stability and security; implement to support the heterogeneous and cross-platform database. At the data transform process, use the combined configurable file to explain the data transform flow, make the data transform process highly flexible and easily designed and modified. The ETL system was put to test, which proved that: The program is indeed feasible, the development process is simple and easy to control and the development cost is low. The ETL system has been successfully applied in the real environment of multiple users, and earned the users' appreciation. It improved that the ETL system design and development are effective

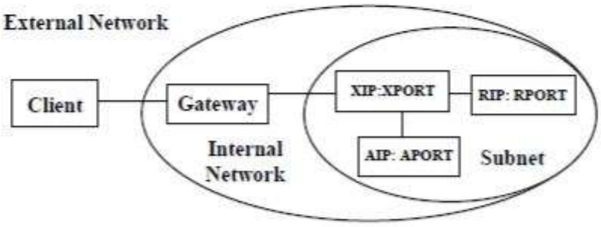

Fig. (5). The network structure of authentication server.

8. PROTECTION STRATEGY OF COMPUTER NET-WORK SECURITY

The network has brought us both the convenience and the network information security issues. Information security issues rise to a very important technology point in the net- work system due to the current computer networks extensive usage, which the computer management explained the con- tent classification, and analysis of the current computer network information security issues, proposed appropriate protection strategies.

Data backup is useful for keeping the data safe in copy files on the hard disk. These files contain the original data that are copied to another place such as mobile hard disk etc., so that the data can be retrieved in case a computer's system is destroyed due to a network virus attack. So, keeping back is one of the strategies to face security issues. Be- sides, good data backup is one of the most direct and most effective measures to solve data security issues. Data backup methods are comprehensive backup, incremental backup, and differential backup. Physical isolation network gateway is to use solid-state switching with a variety of control functions to read and write media to connect two independent host systems information security equipment. Since the host system between two separate physical isolation gateways is connected, there is no physical connection for communication, logical connection, information transfer command, or information transmission protocol. Also, there is no agreement on the basis of the information packet forwarding, but

DOI10.17148/IJARCCE.2017.64160

only data files. On the solid-state storage media there are only two commands, “read "and" write ". Therefore, the physical isolation gateway, from the physical isolation, block everything possible to connect to a potential attack, so that the "hacker" can’t be invaded, and there is not attack that can’t be destroyed to achieve real security.

A firewall is the software located between the computer and the network that it is connected. The inflow and outflow of all computer network communications have to go through the firewall. Firewall network traffic flow through it to scan, which can filter out some of the attacks. In order to avoid its being executed on the target computer, firewall cannot only turn off unused ports, and can prohibit specific port out of communication blockade Trojans. Finally, it can block access from a particular site, thus preventing all traffic from unknown intruders, largely to protect the security of the net- work. Network security encryption key, as a system security, is one of the important means to achieve network security; that is the right to use encryption technology to ensure the security of information. The data encryption is a process of transforming plain original text data into cipher text and its basic process involves an algorithm which is imposed on the data, making it unreadable piece of code. Cipher text data can only be decrypted or entered into with the corresponding key, which protects the contents from being illegally stolen. Decryption is the reverse process involving encoding the process information into its original data. Another data encryption technology is closely related to smart card technology. The so-called virtual smart card contains cryptographic keys, same as a physical credit card held by an authorized user uses a password registered on the network server. Once the common password and identity in usage are the same, while the smart card's confidentiality is quite effective.

The emphasis should not only be given on the network security and information technology solutions, but also great efforts should be made to strengthen the management and implementation of network management personnel, as many insecurities precisely reflected in the organization of the management or staff job entry, etc. side and, which in turn is a fundamental problem for which computer network security must be considered. So, in order to take a practical approach towards strengthening management, establish a chapter to enhance security awareness of the internal staff. In short, there are quite a lot of measures recommended to address the network security issues among which one or several of them are very difficult to solve network security problems. It therefore still needs to work on full and multi-level security measures to maximize the safety and reliability of the net- work system and to make it more secure a service for every- one to make a detailed network based on the actual situation.

9. CONCLUSION

With the continuous development of the network, computer network information security and protection is also beginning to be a widespread concern and attention. Based on the analysis of network information safety factors, this paper put forward a common computer network information safety protection strategy. Besides, the development of the network information safety was prospected and the network information safety protection system was formed. As per our proposed strategy, the use of a certain kind of protective measures alone can’t ensure the network information security. We must use a variety of protection measures, in order to establish a comprehensive network of information security protection system for public companies; we try to ensure the maximum network information security by minimizing the possibility of hacking.

REFERENCES

[1] A Hess, and G. Schafter, “Realizing a flexible access control mechanism for active nodes based on active networking technology,” In: IEEE International Conference on Communications (ICC 2004), Paris, France, 2004.

[2] Testa Bridget Miatz. Zig Bec: “Remote control euphoria,” Telecommunications (Americas Edition), vol. 38, no. 10, pp. 10-11, 2004.

[3] C.L. Abad, and R. Boni, “An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks,” 27Th International Conference on Distributed Computing Systems Workshops, Toronto, 60 2007.

[4] Z. Trabelsi, and K. Shuaib, “A Novel Man-in-the-Middle Intrusion Detection Scheme for Switched LANs,” International Journal of Computers & Applications, vol. 30, no. 3, pp. 234-243, 2008.

[5] Biju Isaac, “Secure ARP and secure DHCP protocols to mitigate security attacks,” International Journal of Network Security, vol. 8, no. 2, pp. 107-118, 2009.

[6] Y. N. Sung, D. Kim, and J. Kim, “Enhanced ARP: Preventing ARP Poisoning-Based Man-in-the-Middle Attacks,” Communications Letters, IEEE, vol. I4, no. 2, pp. 187-189, 2010.

[7] T. Alok, V. D. Sreenaath, and R. Sekar, “Fast Packet Classification for Snort by Native Compilation of Rules,” In: 22nd Large Installation System Administration Conference (LISA' 08), pp. 159 -164.

[8] C. Matthew, “Mobilizing the Library’s Web Presence and Services Student-Library Collaboration to Create the Library’s Mobile Site and iPhone Application,” The Reference Librarian, no. 52, pp.27-35, 2011.

[9] C. Daniel, “A Mobile Strategy Web Developers Will Love,” Computers in 1ibraries, no. 5, pp. 24-26, 2010.

[10] B. T. Johnstone, “Boopsie and Librarians: Connecting Mobile Learners and the Library,” Library Hi Tech News, no. 4, pp. 18-21, 2011.

DOI10.17148/IJARCCE.2017.64160