Computer Database Security Management Analysis and Discussion

Kai Hu[1,a]

[1]Wuhan City Vocational College, Wuhan, Hubei, China

[a]wgyhk@126.com

Keywords: Computer database, Database security, Security management, Security mechanism.

Abstract. Human society entered the 21st century, the Internet and mature technology of the database has been an unprecedented development, security issues have always been a computer database security and database data loss problems are hacking seriously affect the database, for database security Research management becomes extremely important for computer data security issues to further strengthen the strong, we have been now become a large-scale computer information system construction in which an extremely important issue. This paper focuses on environmental factors among computer security threats faced by the database that were analyzed, and thus a comprehensive analysis of the database to improve computer security management countermeasures.

Introduction

With the popularity of Internet **development** in 21 societies of the actual use of electronic space and get involved in more and more enterprises, the central figure among the business gradually turn to the Internet, in the ground of the decentralized departments and companies within the region application requirements and vendor data clearly showing the way for excessive trend in which the database management system gradually extended from single powerful to the entire computer network environment, for the collection and storage and processing and dissemination of data are from the late concentration towards a comprehensive distributed mode [1]. When companies use data path management systems, it is particularly important that the security of database information. The author conducted a comprehensive and powerful exposition.

Computer Database Security Mechanisms

Basic computer database is back-end database computers, plus the foreground program so access control provided for data storage and query and set operations between the information can browse through effective gradually completed. Sharing current information processing computer network environment, a large number of valid data information is the most important feature of a multi-user database exists (shown in fig.1) [2], but at the same time for data integrity and consistency have effective protection, effectively to achieve a minimum level access control.

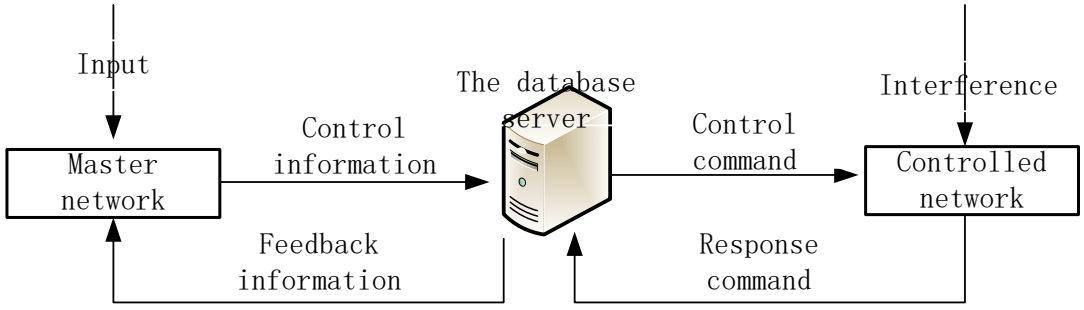

Fig.1 Computer database agency

Two typical pattern computer database used is B / S mode and C / S mode. C / S model used is divided into three layers (shown in fig.2) [1]: a. first is the client,b. application server,c. database server. The main manifestations are by the client to transfer data to the application server and then transmitted to the server database again them.

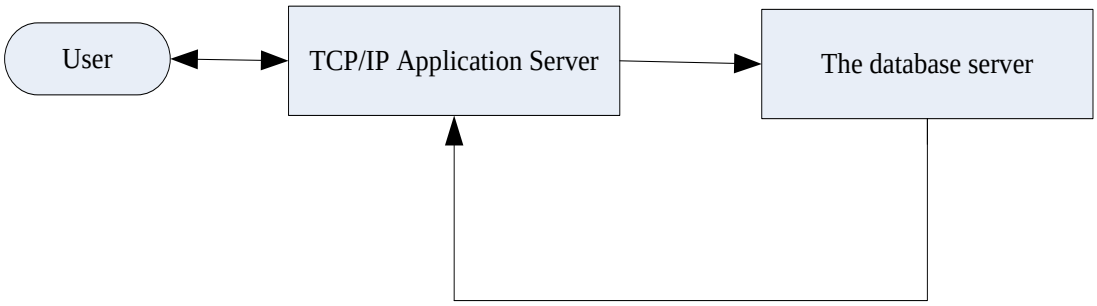

Fig.2 Computer database B/S Mode

B/S model used is **divided** into three main structures: a. first is the browser,b.Web server, c. database server, the main forms described above in Figure 2. From this we can see, both in the computer database schema exists a large degree of common ground on the structure, all of which are related to the computer network and system software and application software.

Layers of Security Mechanisms Described in Detail

Computer network system security mechanisms. If the **database** by external malicious attacks from invading the information, first from a computer network system begins to attack the invasion, so we can determine the first protective barrier is the normal security network system database security [2]. We just stood in technical terms, it can be roughly divided into its anti-intrusion detection and collaborative intrusion detection technology. I do are listed separately below its relevant department explained.

First of all, which computer systems are equipped with a firewall, the firewall has become widely used nowadays one of the most basic **precautions**. The main role is played by a firewall access channel between the network and the network cannot be trusted trusted effective monitoring, the establishment of a barrier to effective protective measures against internal network and external network, the external network which carried out illegal access effective interception and internal information effectively prevent effectively prevent information outflow [3]. For external firewall intrusion prevention have strong control, but for the illegal operation of the network but can not be internally generated block to effective control.

Secondly, with regard to intrusion detection, has grown in recent years, a strong defense technology, which mainly uses statistical techniques and the rules of technology and network communication technology and artificial intelligence techniques and **methods** of effective and comprehensive prevention technology together the main role is played by intrusion detection network and computer system for effective monitoring [2,3], the ability to effectively reflect whether there has been compromised or misused.

Finally, collaborative intrusion detection technology, for lack of independence of the previous point intrusion detection systems and deficiencies in many aspects, collaborative intrusion detection technology have an excellent remedy, which their systems IDS is based on a unified standard, Intrusion information between components are detected **automatically** exchanged effectively [4]. Also, you can check information for effective intrusion by automatic exchange of information, and can also be effectively used in different network environments.

a.Currently, the market is a large part of the computer has **Windows** NT and Unix operating systems, it has the general level of security is in C1, C2 level(shown in fig.3) [4]. The main security technology writer summarized as the following three points:

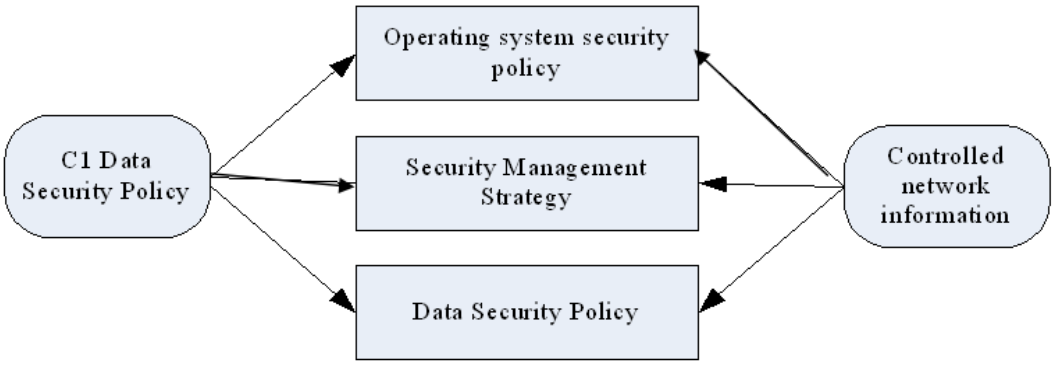

Fig.3 C1 and C2 class server operating system security

b. It is mainly carried out on the local computer security settings configuration, security policy mainly security including password policies and **account** lockout policies and audit policy and IP security policy and a series of security options [5], which can be reflected in the specific application the user's account and password and many other aspects of access to and the like.

c. The main methods and policies for network administrators **to** manage the safety management system to take. Because the operating system and computer network environment is different, so the need to take security management strategy and there are also different methods.

d. This is mainly reflected in the following points: data encryption and data backup and data storage among security. It can be used in technology has a lot of, **which** are: authentication, IPSec, SSL, TLS, VPN and other technologies.

Database management system security. Database systems in which the operating system files are in the form of effective management [5]. So, people **can** invade the database operating system vulnerabilities among them direct steal their database files, you can also take advantage of OS tools to illegal operation and tampering with the contents of the database file. Such risks exist in the user database is generally difficult to rub the sleep, for this vulnerability analysis is considered BZ-level security technical measures. Level database security technology, mainly for the case of the current two levels has been destroyed for effective solutions to ensure database security [5]. So, for the database management system we must require a more robust set of security mechanisms.

The client application security. Important aspects **of** security of computer database client application. That have a strong and relatively quick and easy to achieve its main features, but also to changes in demand based on very easy to make corresponding changes [6]. In addition, for the preparation of the client application also has a greater flexibility.

Using DBMS Security Mechanisms Prevent Network Attacks

There are many large DBMS technology to provide database security, relatively speaking are very sound, but also for improving the security of the **database** also has a significant positive effect [6] (shown in fig.4).

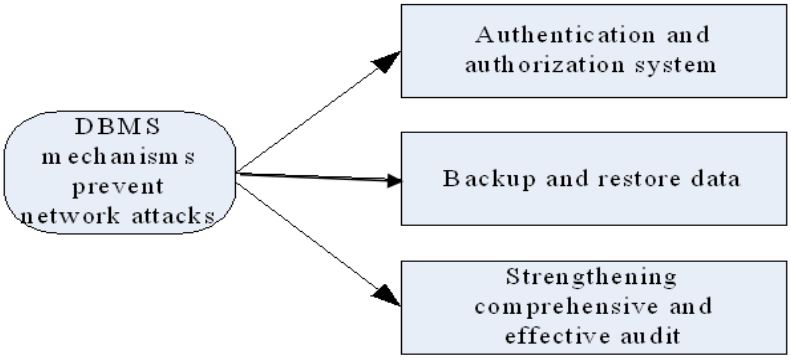

Fig.4 DBMS security mechanisms prevent network attacks

Authentication and authorization system [7]. Certification is the identity of the person or application process requesting service **authentication** system; Authorization is the process of licensing the identity mapping of an authenticated database users have been granted, the process is allowed to restrict user behavior occurring within the database. When SQL Server database server permissions settings, you should set up a separate program for the DPeb a restricted login, specify its only access to specific databases, and add a user for that particular database.

Backup and restore data. When the system can malfunction, an administrator can in the shortest time data through data backup and recovery, maintaining state originally treated for a data integrity and consistency with a powerful guarantee [7]. Usually for database backup usually take the following forms backup forms: First, a static backup; **Second**, dynamic backup; Third, the logical backup. However, for the recovery of the database, you can take a lot of the ways disk mirroring and database backup files and database online logs been effective recovery.

Strengthening comprehensive and effective audit. Through effective audit, the user can perform all operations are among the database can be effectively automated recording, and then the recorded information is stored in the audit log of all of them, **to** conduct a comprehensive audit can effectively enhance the use of tracking information, will the current status of the database a series of events are sufficient to reproduce [7]. Therefore, we can effectively identify illegally accessing data and the timing and content access information.

Conclusion

Modern society is in a stage of evolving computer information technology also has an unprecedented development. However, the continuous rapid development of Internet technology, the security of its computer database is the main problem today's evolving, with the continuous improvement of modern means of network intrusion systems**,** security technologies it uses are constantly further improved. Only problems that arise for continuous analysis and research, lessons learned and then deal with a range of comprehensive and effective new problems arise. In short, security is a new era of computer database permanent important issue, only a comprehensive security through reasonable means of science as well as continuous improvement and perfection in the latter part of the development process, we can better secure the system effectively improve reliability.

References

[1] X.L. Dai,Based on SQL SERVER database of network security management, Network Security Technology and Application, 2009 (04).

[2] N.Y. Wang, L.F Li, Application security awareness and computer databases, Southwest Medical, 2009 , pp.34-38.

[3] G.J. Xi, T. Zheng, Database Security Mechanism C/S Structure. Educational information, 2004 (09).

[4] Y.F. Xue, L.J. Qiong andY.J.Li,Research database security and protection of technology, China New Technology and New Products, 2011 (03), pp.54-58

[5] Sh.Z. Zhou, Talking about database security research and applications, Computer Knowledge and Technology. 2010 (05).

[6] H. Wang, M. Fang and R. Li, Analysis and model of the network database security issues, XI'AN PETROLEUM INSTITUTE (Natural Science). 2003(6), pp.231-239.

[7] J.M. Liang,Safety factor network database analysis and prevention in optical disc technology, 2008 (09)