Research and Improvement on PXE Security of Dynamic Distributed Network of Non-Fixed Disk

Huang Guanli
Beijing Vocational College of Electronic Science,Beijing, China
Email: huangguanli@dky.bjedu.cn

Yang Bin
Dept. of Electronic and Information Eng., Beihang University, Beijing, China
Email: mhi2008@yeah.net

***Abstract*— PXE(Pre-boot Execution Environment) tech. has played great roles for the powerful compatibility and ease for maintenance. Internet requirement for data safety are more and more important while PXE methods is lacked. The applies diskless tech and dynamic distributed security system on data storage has been analyzed. According the PXE tech. improvement and design thus reduce the risk of letting out and dependability of the network data under the strict data management. The function may bring huge economic benefit with the popularization of the applications and low maintenance cost.**

***Index Terms*—PXE(Pre-boot Execution Environment), anthropic factor, diskless network, SIMS (Secure Information Management System)**

I. INTRODUCTION

Storage security of business sensitive information, such as: privacy information of bank customers, credit records, teaching records of educational institutions, business customer information, consumption records and tax declaration information and so on, takes up 80% of security problems. With current security protocols of Internet, these sensitive information could be effectively protected during the transferring stage. However, how to protect them during the storage stage has become a critical issue concerned by companies. Competitive environment of globalization triggered the evolution of business processes from traditional paper-based business processes to more efficient computer-based business processes of the domestic firms in China, therefore the requirement of the security storage of business information is increasing..

A. Key issues analyzing of PXE data security

PXE data security is, essentially, the network information security. Specifically, it is a protection of hardware, software and data of network system from interruption by accidental or malicious destruction, change and disclosure in order to maintain continuous and reliable operation of the system. Generally speaking, PXE data security includes all of related technologies and theories which deal with information confidentiality, integrity, availability, authenticity and controllability in PXE network. Due to diversity of network connection, uneven distribution of terminals and characteristics of openness and connectivity, PXE network is vulnerable to be attacked by hackers, malware, viruses and trojans. How to protect data stored in the network emerges as a critical problem, while the security of storage, transmission, management and backup of the network data has attracted more and more attention of researchers as well. How to effectively protect critical information and data and improve the security of computer network system have become a critical issue which requires to be considered and addressed for all computer network applications. There have been a lot of solutions for strengthening the security of network data; however, all of them have flaws. Although lots of companies protect their data relying on database security technology, the database can not afford to store all of information and data. Besides, there are many information and data which are not necessary to be stored in database, and will seriously affect the efficiency of data storage. Therefore, the solution of storage security must be one of the hot techniques in the future.

According to the development trends of network storage market and progress of the related techniques, network security storage market definitely replaces the traditional network storage market. Based on the PXE diskless network technology and dynamic distributed data storage, this work focuses on strict protection of sensitive data without effecting use, which could achieve the comprehensive network data security storage.

Currently, the PXE data security mainly relays on the related hardware and software supervised by human. There are relatively large numbers of management software which can be roughly classified into two groups: the one is used for network management and monitoring, in order to protect the network, monitor the undergoing system software, and manage the access devices of the network (such as firewalls); the other is used for data management and backup including data encryption, transmission, and backup processes (such as the majority of the encryption software and redundant backup

doi:10.4304/jcp.7.7.1681-1687

systems). There is a lot of hardware which could provide the similar functions as well, such as hardware firewalls, hardware dongle, etc.. However, all of the tools mentioned above require to be supervised by specifically trained human. Due to the different quality of PXE system users, the protection of PXE system and data is always stopped by personal reasons for which instance users usually close the firewalls. Moreover, different standards between internal and external system also make the security of system ineffective. According to recent reports, sensitive data leakages are mostly caused by personal error operating and low awareness of protection. They are even not aware of their confidential data being exposed to hackers and other illegal intruders. The emergence of situation mentioned above is mainly due to the imperfect combination between security management and control of the majority of data security systems, currently. In order to solve these problems and reduce data leakage occurring, this paper proposes an approach to construct a PXE based data security system to meet the storage security requirement.

B. Related information systems with storage security

In this section, related information systems with storage security will be introduced and analyzed.

Encrypted File System (EFS) mainly runs in the Windows 2000 and Windows XP. It could encrypt data of the file system, so that only the file creator and owner can access the file. This system has relative reliable security, but can not provide multi-user file sharing.

Self-Certifying File System (SCFS) was proposed by New York University in 2000, which achieves authentication of client at system server. They also presented a variety of effective authentication approaches. However, this system did not provide authentication to costumer of server and information security assurance.

Fast and Secure Distributed Read-Only File System (FSDROFS) proposed in 2001, has not yet entered the product development stage. The system proposes an approach to make signature for entire file system, thus each reading file has a signature correspondingly. Even if the signature file has been stored at some distrustful hosts, it can not be tramped. However, this file system only provides file reading function, but not modifying function.

Secure Information Management System (SIMS) is a key product of a large information security project. SIMS achieves to provide the information storage and data access authorization successfully at different computers individually: file server and key server. All information is encrypted and stored in the file server. The key server will check file access permission and transmit the result to the file server. The main purpose of SIMS is to distributed share data between multi-entry (individual user or company). The key server centralized controls information access permissions and encryption keys. Therefore, key management cost is relatively low of the system at trusted hosts so that relative less number of human is required to maintain the security part of the large system.

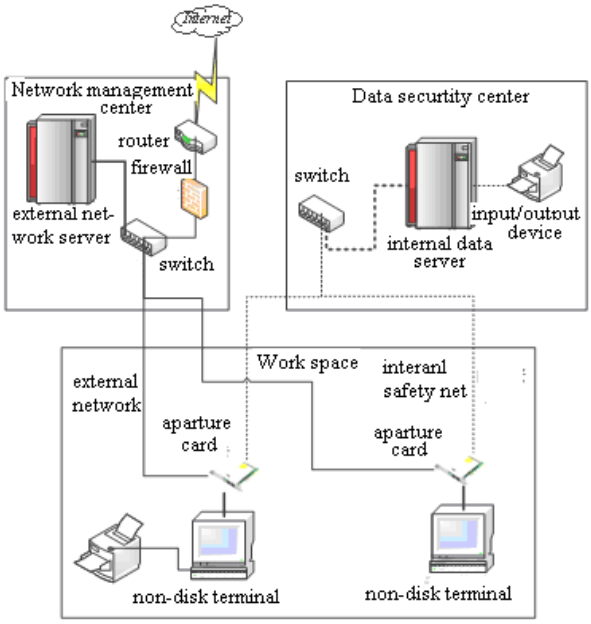

Figure1.The topology of diskless network

However, the centralized structure of the key service is easy to make the key server of entire system becoming bottleneck of system, which is vulnerable to be attacked by Distributed Denial of Access Service (DDOS) attacks [1, 2].

II. CONSTRUCTION AND CHARACTERISTIC OF DYNAMIC DISTRIBUTED PXE NETWORK DISKLESS DATA STORAGE

A. Construction of dynamic distributed PXE network diskless data storage

Dynamic distributed network diskless data storage is one promising technology of data storage. Its platform is a distributed file storage management platform, which provides storage encryption and dynamic distributed authentication in order to improve the certification efficiency and high attack resistance. With the distributed data storage, it could achieve the data off-site backup, and more security, integrity of information storage solutions. The platform consists of four systems:

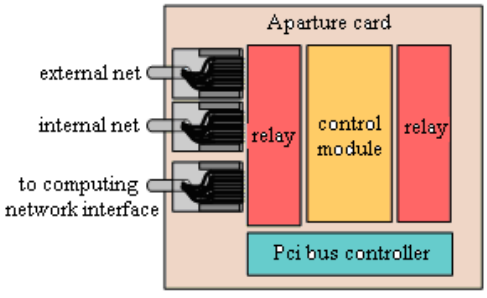

Figure 2. The principle of aperture card

Storage encryption system for application files: It could provide many security mechanisms such as: encryption of independent evaluation, digital signatures, access control, data integrity, traffic filling, routing control, notarization, identifying and auditing etc., and corresponding security management solution for remote user accesses.

User identifying system: With PXE platform, identification server strictly operates identification processes and access control, when remote user access sensitive applications.

Security Application Server System: It consists of key management center, access control center, security identification server, authorization server, etc., which is in charge of access control and security management activity, such as production, change, configuration, and destruction of the keys, certificates and other security materials. It bases on PXE technology and could achieve remote control.

Distributed key storage system: It employs the PXE diskless storage technology, with distributed storage, anti-listening, anti-interception ability. Besides, it can protect confidentiality and integrity of information from active or passive attacks, such as tampering, deletion, insertion, replay, code-breaking of plaintext key etc.

B. Characteristics of dynamic distributed PXE diskless network data storage

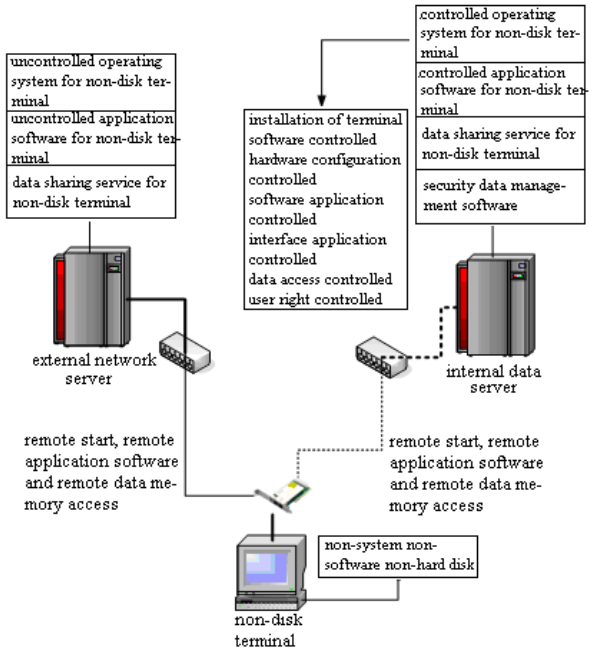

Figure3. System software configurations

PXE (Pre-boot Execution Environment) was designed by Intel with which user can start the computer through network. Protocol consists of two parts: one is designed for client and the other for server. Since the first running and successful remote booting of Windows 98, this technique's reliability and stability have been improved continuously. Until now it has achieved diskless operating at the majority of systems, such as Linux, DOS, WIN2003, WIN VISAT and all series of Windows operating system.

PXE is an upgrade product of RPL, it provides two means to start system: one employs the DHCP mode with dynamically assigned IP, the other employs BOOTP mode with fixed IP. Communication protocol is TCP / IP which guarantees the efficiency and reliability of the connection with Internet. The process of PXE diskless workstations boot are as following: Firstly, Bootrom takes over system boot right after client powers on, and sends BOOTP / DHCP request to obtain the IP through broadcasting in which the client's MAC address is included. Secondly, the server sends IP address, default gateway and boot image file back to client after identifying the MAC address. Thirdly, Bootprom downloads the boot image file from the server under TFTP protocol. Then, the client could be booted by the boot image file which can be a simply boot process code or an operating system. The boot image file could create a virtual disk at the memory of workstation. With this virtual disk the client can boot and connect to the server, the preference environments (such as the path of operating system, related modified registry) of diskless boot can be imported from server [3].

Since PXE can support multiple operating systems, the majority of application software can be employed perfectly. The applications of client only run at its own computer without occupying the server resources, thus the server can operate more than 100 workstations at the same time. Once operating system and application software have been installed at the server, no matter how many workstations there are, with the same configuration of hardware there is no need to reinstall the software and system. The maintenance and operation are convenient, for instance, when software have upgraded, user could upload the new system to server. Then all workstation's software is upgraded. Moreover, it provides more reliable data storage and application management which achieves much more efficient security management of PC.

III. THE DYNAMIC DISTRIBUTED PXE NETWORK DISKLESS DATA STORAGE SYSTEM

A. The separation of PXE information storage and access authorization

The PXE-based dynamic distributed diskless data storage system employs the SIMS technique and achieves information storage and access authorization independently at individual server host: file server and key server. All of information are encrypted and stored in the file server. The key server will check file access permissions and transmit the results to the file server. The main purpose of SIMS is to distributed share data between multi-entry (individual user or company). The key server centralized controls the information access permissions and encryption keys.

Therefore, key management cost is relatively low of the system at trusted hosts so that relative less number of people is required to maintain the security part of the large system. Dynamic distributed diskless network data

storage system achieves two-direction authentication between client of system server and user of server and employs various effective authentication mechanisms. This system also refers to the FSDROFS technology and employs the approach of generating signature for entire file system, thus each reading file has a signature correspondingly. Therefore, once the signature file has been stored at some distrustful hosts, it can not be tramped. Moreover, the file system could also have access to reading and modifying the file.

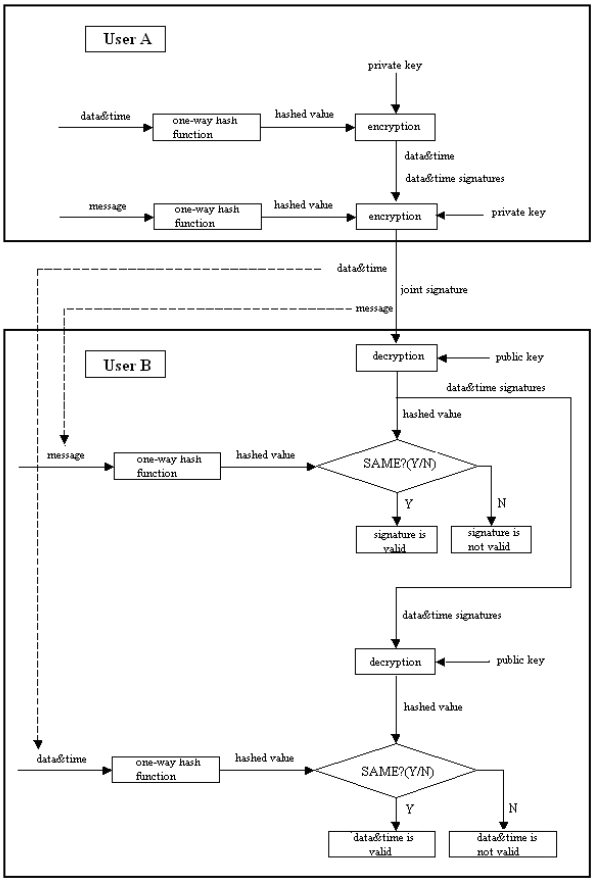

Figure 4. The flow chart of digital signature with public key cryptography, one-way hash function and time-tag

In the dynamic distributed diskless network data storage system, security solutions employ Distributed Secure Information Management System with Split Secret Sharing (DSIMSwSSS) to resolve existing security system defects. The main idea of distributed key storage technology is to decompose the key into n fragments with checking part and store them in n hosts respectively. Users are only required to obtain m fragments back from hosts (m<n), they are able to reconstruct the key and get the certificates. Unless the number of fragments obtained from hosts is less than m, the key can not be reconstructed, thus users are not able to access to data file. This system requires all servers to maintain an encrypted file access control list (ACL). When a user requests to access specific document, server will compare user's information with the ACL before responding the request. In order to operate the ACL, it requires a synchronization mechanism. With DSIMSwSSS technology, the security and stability of system are improved, and it greatly increases the capability of system's fault tolerance. For example, even if there are d hosts with error or even unable to provide services, as long as d <n-m, user still could obtain the key from other hosts and access data file.

B. Construction of diskless network for data security

Improving the data security by diskless technique to construct the quality diskless network: As illustrated in Figure 1, the network system is distributed at data security center, network management center and work area respectively. Data is divided into two parts, namely, security data and common data. Security data are stored in server unconnected with outside world, while common data in server which is able to access Internet. With traditional protection approach, the client does not store any data, it could only access server to get on-demand data. Data security center possesses internal network data and remote boot server. The terminal does not equip storage devices (such as disk), or install any system and application software. All of data and operating system are stored in server. The entire internal network disconnects with Internet physically. Network management center possesses external network data and remote boot server. The terminal does not equips storage devices (such as disk), or install any system and application software. All of data and operating system are stored in server. The entire external network connects with Internet so that the terminals of external network have access to Internet.

TABLE I.
Requirements of Different Algorithm

algorithm	applications	requirements
asymmetric algorithm	key exchanging and data signature	process complexity $\geqslant 2^{512}$ public key is deducible public/private key pairs are deducible Speed≥RSA algorithm
symmetric algorithm	encryption and decryption for keys	process complexity $\geqslant 2^{64}$ Speed≥DES algorithm
one-way hash function	hash computation for documents	process complexity $\geqslant 2^{128}$ Speed≥MD5 algorithm

The terminal can both connect to internal or external network by aperture card. Internal network is separated with external network physically. The user could process the security information when terminal are connecting with internal network and surf the Internet when terminal connecting with external network. Aperture card is designed based on relay control technology which could ensure the physical separation of internal and external network. The principle of aperture card is shown in Figure 2.

Characteristics of the entire network: Terminal does not equip with storage devices (such as hard drives, etc.) and does not install any operating systems and application software; When terminal accesses to the network, it can automatically obtain the appropriate network operating system and application software; Terminal supports personalized configuration; Terminal has more efficiency appliance, convenience, stability, manageability; Terminal can switch easily between a varies of operating systems, and it can also achieve to provide multi-group application environment;

More reliable data storage and application behavior management is provided, and a more effective safety management system for internal PCs is achieved; Unified arrangement of systems and software is provided, which completely replaces the old software distribution; Each Wing operating system on each server can manage up to 100 PC terminals and, simultaneously, workload of people is dramatically reduced; Standard PC can reach PC 100% performance of computing capability which could efficiently run large software and computing based software; The compatibility of standard PC makes it possible to sustain DOS / Windows / Linux / Unix and other operating systems, and a variety of application software and peripherals; Standard management system could coexist with existing management systems and management software to improve management efficiency.

C. The notion of system configuration and data managment

Software architecture of system is shown in Figure 3.

When terminals access external network, traditional approach can be used and special control software is unnecessary, since there is no security data to protect.

When terminals access internal network, network data could be efficiently protected by data management system. The data management system includes several modules as following:

Operating system management and control of terminal: Managing and controlling operating system of each terminal in order to prevent any changing of authority in system by users. Software installation management and control of terminal: Installing or uninstalling application software should be under control of server in order to ensure that unauthorized users can not change system. Hardware configuration control of terminal: All of hardware devices of terminal are supervised by server in order to prevent data from being changed by user through access port of terminal.

Network's devices access control: Network's devices (such as terminals, printers, etc.) must be authorized before accessing network data, while unauthorized devices could not allow to access. Software utility control of terminal: All of software at terminal assigned limits of authority, only user with permission could have access to use. Besides, user with low-level permission can not use software with advanced security level. User Authentication: Authenticating user of network. Non-authorized users can not access network.

Access control: Each user can only access data with their corresponding permissions, which means that they can not access data out of their security limits. Audit records: Recording user's activity such as devices accessing, user accessing, system operating etc. Flexibility of the utility: Isolating protected data from external network so as to increase flexibility external networks. Data backup and encryption: Employing hardware and software technology to backup data in real time to achieve reliability of data storage; encrypting data during storing and transmitting with proper methods in order to ensure data security. Data access limitation control: The data required to be protected are stored and managed centrally; users can only have access to get data based on their authority, while data beyond authority limitation is unable to access.[4]

IV. STORAGE SECURITY SOLUTION WITH TIME TAG

A. SIMS A comprehensive improved of SIMS refered to digital signature technology

PXE key server achieves distributed management; thereby system efficiency and security are enhanced. Conventional digital signature based on symmetric cryptographic algorithm is to sign data with symmetric cryptography system and arbiter. Digital signature based on symmetric cryptographic algorithm has many shortcomings: it is very time-consuming for the arbiter. It requires being equipped with database which will be bottleneck of software system. Moreover, database must be completely secure, or there will be false documents. Therefore, digital signature with symmetric cryptography system and arbiter hardly ensure data security. Digital signature based on asymmetric cryptographic algorithm is to sign data with public key cryptography. In some public key algorithms, both public key and private key are able to be used for encryption. However, digital signature based on asymmetric cryptographic algorithm also has shortcomings, such as: 1) High time-consuming for large files can not meet time efficiency requirement; Signature of user may validate all time which may lead to a situation that a user can withdraw money at any time with same cashier check. Obviously, it is not permitted. In view of shortcomings of those algorithms, digital signature technology of dynamic distributed diskless network data storage system is more inclined to use time tags and one-way hash function to solve data storage security.

Based on control timing of diskless technology, digital signature of PXE dynamic distributed diskless network data storage system uses time tag (also known as timestamp) to attach date and time information with messages. Thus, the signature file can not be duplicated. Hash function is a mathematical function with which variable-length input string (called pre-mapping) can be changed into a fixed-length output string (hash value). One-way hash function is a single-direction hash function. It is easy to calculate hash value from value of pre-mapping. However, the opposite, to obtain value of pre-mapping from hash value, is very difficult [5].

B. Digital signature with public key cryptography and one-way hash function

As shown in Figure 4, digital signature solution of PXE dynamic distributed diskless network data storage system offers data authenticity, non invasive, repudiation and non-duplicate [6].

*A*lgorithm demand and analysis :PXE dynamic distributed key storage system employs distributed storage security system to strengthen overall security, which does not need to investigate data encryption algorithm. The system opens storage access layer to associate with varies of encryption interface in order to achieve different encryption approaches management and conversion at the same system. For instances, symmetric encryption standard DES, 3DES, IDEA and widely favored AES; non-symmetric encryption standard RSA; VPN standard IPSec; transport layer encryption standard SSL; secure email standard S-MIME; secure electronic transactions standards SET; through vulnerability description standard CVE. These are all commonly adopted algorithms and protocols after a spontaneous selection process, known as "facts standard." Usually the 1:1 encryption algorithms are recommended so that it will not increase network throughput. When dynamic distributed key storage system employs non symmetric algorithm to conduct data signature and key exchange, algorithm complexity is required for no less than 2512, pairs of public key and pairs of public private key are deducible, and algorithm speed is not slower than RSA. When system uses symmetric algorithm to protect the pair of public and private key and user information at memory card, algorithm complexity is required for no less than 264, and the speed is not slower than DES Algorithm. When system employs hash function to guarantee integrity of signature document and information at Memory card, algorithm complexity is required for no less than 2128, and speed is not slower than MD5 Algorithm. As shown in Table 1.

Security of algorithm depends on the key, and good keys interpret those random bit string generated by automated processing equipment. If a weak key generation method is employed, whole system would be weak in security. Many encryption algorithms have weak keys. Thus before using specific encryption algorithm, we need understand the weak key algorithm with algorithm instruction. We must prevent the weak key generation. There are many ways to transfer keys. The initial off-line products are not related to key transferring. ANSI X9.17 standard presents two kinds of keys: encryption key for keys and encryption key for data. The second on-line products need to transmit public key by network, it can use key's encryption key to encrypt the data key or key transport protocol of public key cryptography system to transfer the key. Public-key cryptography has a flaw, that is, if user A's public key has been replaced by C, user B is difficult to detect. Therefore it requires for adding checksum for all keys at the memory card so that one-way hash function needs to compute all keys respectively.

PXE dynamic distributed key storage system usually does not employ software encryption (encryption algorithm with software). Because encryption process is performed in local computer, attackers can check the memory and analyze algorithm to break the algorithm. Therefore, dynamic distributed storage system typically uses hardware to perform algorithms, with which encryption and decryption are both carried out in hardware to guarantee the security; attackers are not able to track. The approach of using control keys in system are as follows: each key appends a control vector which is used to indicate usages and limitations of the key. Firstly, taking a one-way hash computation with the control vector, and then XOR with the master key and encrypting the session key with the results. At last, it stores the encrypted session key and control vectors together. When reconstructing session keys, it requires for doing a one-way hash computation with vector control, and then XOR with the master key, the decryption can be achieved by the results. In addition, keys will be immediately destroyed from the machine after usage. The disk will never store keys. If user wants to update user's keys, the system must firstly recover the old key. If the old key is correct, a new key is provided to the user. The old Key will be destroyed immediately.

V. PROSPECTS

As mentioned above, PXE dynamic distributed diskless data storage security solution is based on comprehensive improvement of SIMS and referred to advances of digital signature and diskless network technology. With distributed data storage, it could achieve data off-site backup and distributed management of key server to improve efficiency and security of entire data storage system. The end users of the PXE-based dynamic distributed data storage system are highly developed information businesses: securities, insurance, banking, education, transport, tourism, Internet, telecommunications, large-scale retail enterprises, membership-based industry, pharmaceutical company's internal information platform, e-government, and other public information service. Data storage security is a matter of national security and social stability which includes network technology, encryption technology, information security technology, applied mathematics, information theory and other disciplines. To ensure reliability of information security, it is imperative to develop security storage products with independent intellectual property rights. This paper proposes an

approach to improve network data security which employs the latest dynamics distributed storage technology and PXE diskless network technology to integrate all of network data and operating systems on single server, so that centralized data storing and managing are achieved. This approach reduces risk of data leakage from three aspects: network edge security, data transferring security and data storage security. It solves management loopholes from technique ways and provides reference for how to effectively protect network data and ensure data security. With popularity and business application of this outcome, it has substantial economic value.

ACKNOWLEDGMENT

This work was supported in part by the 2010 Scientific Fund of Beijing Education Commission （ ITEM NO. KM201000002002).

REFERENCES

[1] Pradeep K.Sinha, *"Distributed Operating Systems"*, IEEE Computer Society Press, 2000.

[2] Paul Garrett, *"Making,Breaking Codes "*, Prentice-Hall,2001.

[3] TAN Xiao-dong, *"Study and Realization of Network Clone Based on Pxe,"* Computer Knowledge and Technology, China, Vol. 5 (21), July, PP.5691-5692,2009.

[4] Huang Guanli, *"Implement and Improvement on Data Security Scheme of Dynamic Distributed Diskless Network Storage "*, Computer Science, China, Vol. 36 (4B), April 2009, PP.76-79,2010.

[5] Zheng Yu, MA Weiyin, *"Method on Computer Virus Protection Based on PXE Technique,"* Computer and Modernization, China, NO.164, (04), PP.17-19,2009.

[6] Huang Guanli, *"A Security System Design of Digital Signature Based on PKI"*, Computer Security, China, August 2008, PP.78-80,2008.

Huang Guanli female, born in 1975, Associated professor of Beijing Vocational College of Electronic Science, Master's degree with the major of computer science. Participant Leader of Beijing Quality Course on Network development and the Committee member on China Computer Federation. She published widely, such as academic articles in Computer Engineering and Applications, Computer Science etc; her research interests include algorithm design, Computer Education etc; and has won one National Patents and has published over twenty academic articles as the first author, two of which are EI Indexed. At present, Ms. Huang also undertakes some items, such as Research and Development on Dynamic dispatching GPS system of the Adaptation Road Condition of the Beijing Education Committee Scientific Project. She is also the Participant of Simulation Platform of Small Hybrid Vehicle Control Based on dSPACE of the Beijing Science and Technology Innovation Platform Project, and Practice of School-enterprise Cooperation Mechanism and Platform based on Diversification of the Beijing University Education Reform Projected. Her research Directions are data analysis, signal control, information security, education management.

Yang Bin a graduate student at Beihang University, Male, born in 1985 and received his bachelor degree in Electronic Information Engineering from Beihang University. Currently he is a graduate at Beihang University, majored in Communication and Information System. He will graduate in Jan., 2011. He has accomplished six projects in the field of stereoscopic imaging, video compressing, and audio signal processing and human-computer interaction, such as Stereo Video System, Real-time Audio Signal Analyzer and so on. Besides those projects, he published two papers on mathematical modeling and was awarded Meritorious in the Mathematical Contest in Modeling. He researches on non-overlapping multi-camera tracking. His research interests include computer vision, artificial intelligence, multi-camera tracking, and surveillance. His research interests include multi-camera tracking and computer vision.