Chapter 90
The Implementation with the Network Data Security on the Secure Desktop

Yi Liao and Xiao-Ting Li

Abstract Nowadays, the electronic power industry is improving the level of information, and the data security of the internal network is arousing more and more attention. The domestic units and enterprises implemented relatively comprehensively. Most of them deployed firewall, intrusion detection and vulnerability scanning systems which allow them to reduce the risk of network boundaries greatly. However, as to the network terminal management within the network of the enterprise, the current risk prevention measures are far from enough because the internal network security issues come out easily. Combined with the extensive practical application of the electric power enterprise, this paper puts forward the secure desktop idea so as to solve the terminal security of the internal network computers. This measure can achieve the aim of a further control of the terminal security of the internal network computers. Thereby, it realizes a better controlled data security within the internal network and provides a good security network solution of the protection with the electric power business.

Keywords Secure desktop · Internal network security · Computer terminals

90.1 Introduction

With the technology of computer network, digital communication and virtualization technology are developing fast, the level of the application of information network technology is extending, the applied business system of the electric power enterprise is keeping increasing, and the applied system of enterprise has been networked and infomationization. As the large enterprise may be related to the

Y. Liao (✉) · X.-T. Li
Information Technology Center, China Nuclear Power Technology Research Institute, China Guangdong Nuclear Power Holding Co. Ltd, Shenzhen, China
e-mail: liaoyi2010@cgnpc.com.cn

W. E. Wong and T. Ma (eds.), *Emerging Technologies for Information Systems, Computing, and Management*, Lecture Notes in Electrical Engineering 236, DOI: 10.1007/978-1-4614-7010-6_90,

national secret-related system, the data transmitted may involve the information that related to the safe of country and the life of people so that it should be kept secure and strictly prevent from letting out. As we can see that the security of the internal network is influencing on more and more extend field, the security of the computer terminal is attaching much more attention [1].

The secure desktop idea provides a relatively good solution method which is being used more and more aboard in the electric power enterprise. This paper will introduce the technology of the secure desktop and explain how to apply the secure desktop technology on the computer terminal of enterprise so to achieve the aim of keeping the security of the internal network of enterprise.

The structure of this paper is as follows: Sect. 90.2 will explain the main threat faced by the current internal network security ; Sect. 90.3 will introduce the basic technology and the concept of secure desktop and the principle of how to execute the control of internal network security while using the secure desktop technology; Sect. 90.4 will introduce the advantage brought by the technology's controlling of internal network; Sect. 90.5 make a conclusion.

90.2 Analysis

The security assurance is always the primary content that should be firstly schemed and established by the builders during the establishment of informationization. Especially, when the government, army, large-scale enterprise develop the informationization construction, they build special internal network that physically separated from the internet, adopt many security assurance system, build corresponding institution of security assurance, even caring nothing about how much it will cost. Meanwhile, the security of enterprise internal network is getting more and more attention. No one hopes that the confidential sensitive information can be leaked out or stolen by others, no matter the nation, government, or individual. However, as the informationization of enterprise carries on, various kinds of accident emerge in endlessly.

As to the internal network, the ordinary security accident can be divided into two aspects. One occurs on the borderline of network, that is, the intrusion came from the outside of the network like the vicious attack, long-distance intrusion, worm virus and so on. The other occurs within the network, that is, the voluntary or passive divulgence by the internal network users. Presently, the domestic units and enterprises are implementing much more countermeasures in the aspect of borderline management. Most of the units and enterprises have deployed firewalls, intrusion detection and vulnerability scanning systems which highly reduced the risk of network borderline in the enterprise. However, these measures are far from enough on keeping security. It is suggested by investigation that the proportion of security accident happened at the borderline and internal network reach 42.86 %, among which more than 50 % information risk come from the inside of enterprise. We can say that the threat brought by the abundant computer terminal is much more terrible than that come from the outside as the scale of terminal computer is becoming bigger and bigger [2].

By analyzing the current security accidents, we can find that the main reason is the erroneous operation by the terminal users, especially the cross usage of removable mass storage device among the internet, internal network, even secret-related network, which resulted that the secret-related information should be restricted strictly in the internal secret-related system may be leaked by internet. A mass of facts suggest that, for the general shortage of knowledge and skill among the ordinary terminal users, the document is processed and stored directly on the personal computer terminal. Some temporary file and information of buffer will be produced, which become the source of leakage. What's worse is that it can hardly be controlled for the broad distribution of the terminal. For those reasons, there is no time to delay to strengthen the protection of terminal.

90.3 Principles and Models

90.3.1 The Concept of Secure Desktop

The secure desktop is a kind of technology based on internal network security management of enterprise computer desktop. Its function can be divided as application policy management of desktop, long-distance desktop maintenance, network access policy, removable mass storage device management, uniform distribution of system patch, capital management and so on.

The secure desktop technology roots in sandbox model, which primarily be invented by GreenBorder Company. And it was purchased by Google in May 2007. After that, this patent was applied in the development of Chrome browser. Currently, the application of the secure desktop technology is mainly used to keep the security of operation system, and prevent from the infringement of virus program [3].

90.3.2 The Principle of the Secure Desktop Technology

Using the sandbox technology and the virtualization technology, the secure desktop technology establishes a virtual "container" and makes the users stay in the "container" so that the users' operations of document and registry database are virtualized. When users exit from the "container", the modification made in it will all be reduced. The design mode is equal to running the program in the virtual container, protecting the bottom data by loading the drive of its own, which belongs to the drive level protection.

Besides, the secure desktop technology combines a serial of regulations (network regulations, authorization regulations and so on) to control the authority of users' operation in the "container".

90.3.3 How the Secure Desktop Technology Realize the Security of Internal Network

Establish another desktop under the system, namely the secure desktop. The operations on this desktop are virtualized, that is to say, the secure desktop is equal to sandbox container. During the usage, only one desktop can be see, the default desktop or the secure desktop.

Basing on the deep analysis of users' requirement, the secure desktop will be started-up as long as the users log on the VPN and access important resource. This moment, a closed and virtual working environment, namely the secure desktop, will be created automatically by using the virtual technology. All the operations are virtualized and the process within the secure desktop and out the secure desktop are separated. The operations, temporary usage, data received are all redirected (virtualized) and high strength encrypted, because all data are concentrated stored in the server and nothing will be exist on the client. It efficiently avoided the risk brought by the misusage of removable mass storage device, the network attack, and Trojan program.

The secure desktop aim at intercepting and redirecting the aspect (operations may lead to the leakage of data) as follows [4]:

- Forbid using peripheral copy output: include USB, print, COM, CD-RW and so on, so as to prevent from leaking out important data.
- Virtual file operation: the modification of files and system executed by process under the secure desktop will all be redirected and encrypted. The files redirected will all be deleted after exit from VPN and the secure desktop. That's to say, no change or mark will be kept on the default desktop while operating files under the secure desktop.
- Protect the operations of registry database: redirect the operation of registry database belonged to HKEY_CURRENT_USER branch and the key value of registry database belonged to other branches can be read but not wrote.
- Constrain network communication: under the secure desktop, the communication connect outward will be strictly controlled, only the access of VPN network can be permitted, so as to prevent from leaking out the material downloaded by VPN. This constraint contains the follows:
  - Forbid communicating with the local computer: forbid the communication between the secure desktop and the physical desktop, so to avoid saving the important data on the local server.
  - Forbid communicating with local network: in the secure desktop, communicating with other computers within the internal network is forbidden, so as to prevent from transmitting and restoring the important data through LAN.
  - Forbid communicating with internet: in the secure desktop, the usage of network application and leaking out data through network communication are forbidden, so as to prevent from leaking out the important data by internet transmission.

- internal process communication (IPC) filtration: IPC filtration is mainly aimed at cutting board and message. The process within the secure desktop can't send message to the process outside the secure desktop.
- Trace cleanup: after exiting from the secure desktop, all the trace will be cleaned up compulsorily and all the operations will be reduced. Even if the secure desktop get breakdown for power off, the secure desktop will automatically detect and clean up the trace which left behind when started up next time.

90.3.4 The Application Model of the Secure Desktop in the Internal Network Security Management

For example, when a staff needs to log on the business system (like the financial system) to operate business data, he/she can only download the data through sandbox and edit it in sandbox B.

If he/she needs to search related material by Google, he/she can switch to secure desktop A of sandbox A and access the internet in sandbox A.

When he/she want to transmit the data to personal mailbox of internet and treat them at home, he/she can't do it, because accessing the internal network is not permitted in sandbox A, and the data can't be copy to sandbox A, so he/she can't see the data if in the sandbox A.

He/she can't access the network under the default desktop, but can do the daily document maintenance. If he/she needs to access the internet, he/she should log on the virtual desktop A. If he/she needs to handle official business, he/she should log on the secure desktop B. These secure desktop are separated, and data can't be transmitted mutually. We can see from it that the logic isolation among the official network, internet, and the critical business network by using the secure desktop technology [5] (Fig. 90.1).

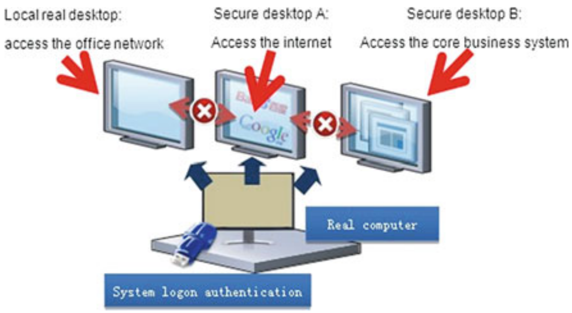

Fig. 90.1 The application model of the secure desktop in the internal network security management

90.4 Advantage

Generally speaking, the secure desktop management system improved the level of security management by using security management information technology, took full advantage of the extant advanced network management tool, strengthened the control of network computer terminal, realized the real time security monitor system, and can make the security-integration with other network security equipment at the same time, which made the internal network become the high speed, secure official network system [6, 7].

The advantage in internal network security management brought by the secure desktop contains the aspects as follows:

- Security: the critical data can only be accessed under the secure desktop, which prevents from leaking out through internet, and keeps the security of terminal.
- Low cost: only virtual security gateway device and authorization and authentication of terminal access should be purchased, and no need to buy another set of network device and official computer.
- Quick implementation: for the original network, there is no need to reconfigure the hardware on a large scale and change the network structure.
- Easy to maintain and upgrade: only virtual security gateway needs to be maintained, only authorization and authentication tool is needed to be accessed when upgrading, and only extra virtual security gateway device is needed to become a cluster when the existent device can’t satisfy the support for the fast development of network [8] (Fig. 90.2).

In view of evaluations on the method, which realizes intranet data security by the secure desktop, and from the respective of practical effect on establishment, maintenance, management, secure desktop to realize data security satisfies the actual requirement on enterprise informationization establishment, and it is suitable for application [9, 10].

90.5 Conclusion

The security protection of personal terminal has aroused general attention among the constructor and IT service providing company. For example, some of the enterprises deployed strong audit system, the double-use monitor system, and the security detection system, etc. In the special network of industry, which somewhat relieved the hidden danger of terminal security. However, these measures were almost realized by installing clients (the principle of it is similar to Trojan program) on the personal terminal forcibly, which brought the terminal users a little worry (it might bring inside secret leakage or exposure of individual privacy) of the administrator department. Thus, it was rejected at different degrees by terminal users when implemented and had limited effect.

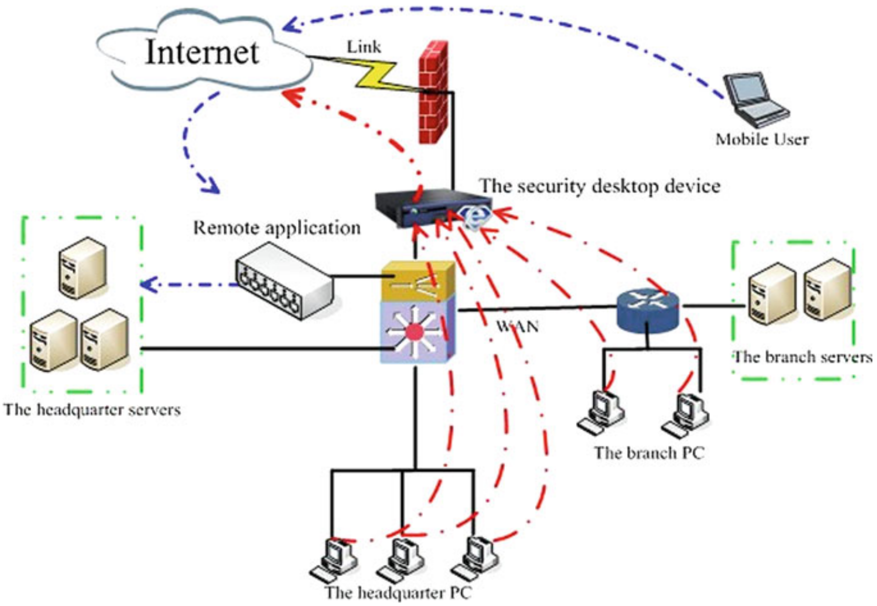

Fig. 90.2 The structure of the secure desktop in the network

As the secure desktop is specially used to protect the access of important resource, the original use habit of terminal users will not be influenced. No additional device or software will be installed in users' terminals. The users can access other resources in the special network as usual, meanwhile, they can access the important inside resources (like the inside official system) securely and conveniently without worrying about leaking out secret by his/her miss-operation and without worrying that the individual information (like personal directory and photo) stored in computer will be collected. Therefore, using the secure desktop technology to realize the security management of enterprise internal network will become necessary in the field of enterprise information security management.

References

1. Zhang, S., Liu, W., Yang, S.M.: Discuss about the green protection strategy of enterprise internal network. Electr. Power Inf. Technol. 3–8 (2008)
2. Pan, Z.Y., Pan, J.Y.: Analysis on internal network safety threat and prevention. Ordnance Ind. Autom. (2008)
3. Pan, Y.X.: The actuality and development trend of desktop security management technology. Inf. secur. Technol. (2010)
4. Hu, W., Zhang, C.H., Liao, W.: Security management function design of computer security defence system. Comput. Engine. Des. 5–30 (2010)

5. Liu, H.Y.: Research and design of security support model in the intranet. Mod. Electron. Tech. 3–20 (2007)
6. Cabuk, S., Dalton, C.I., Eriksson, K., Kuhlmann, D., Ramasamy, H.V., Ramunno, G., Sadeghi, A-R., Schunter, M., Stüble, C.: Towards automated security policy enforcement in multi-tenant virtual data centers. J. Comput. Secur. **18**(1), 80–121 (2010)
7. Berger, S., Caceres, R., Pendarakis, D.E., Sailer, R., Valdez, E., Perez, R., Schildhauer, W., Srinivasan, D.: Managing security in the trusted virtual datacenter. Oper. Syst. Rev. **42**(1), 40–47 (2008)
8. Catuogno, L., Dmitrienko, A., Eriksson, K., Kuhlmann, D., Sadeghi, A.-R., Schulz, S., Schunter, M., Winandy, M., Zhan, J.: Trusted virtual domains—design, implementation and lessons learned. In: International Conference on Trusted Systems. Spring (2009)
9. Adeyinka, O.: Internet attack methods and internet security technology. In: Second Asia international conference on modeling and simulation, 2008, AICMS 08, pp. 13–82 (2008)
10. Kartalopoulos, S.V.: Differentiating data security and network security. IEEE international conference on communications, 2008, ICC'08, pp. 1469–1473 (2008)