Design and analysis of a kind of engineering information security protection system

Zeng Lingdong[1,a], Dong Peng[2,b], Zhu Jingqian[3,c]

[1]Department of management engineering and equipment economics, Naval University of Engineering, Wuhan, China
[2]Department of management engineering and equipment economics, Naval University of Engineering, Wuhan, China
[3]Department of management engineering and equipment economics, Naval University of Engineering, Wuhan, China

Abstract—This paper firstly briefly analyzes the general design principles and special requirements of a certain type of engineering information security protection system. This paper focuses on the analysis of information security technology prevention system design. This paper is based on modern information technology and fully adopts the latest development and concepts of information security protection technology; The design analysis process makes extensive use of computer, network security, automation, industrial control, and other technologies. The purpose of this paper is to make a certain engineering and weapon equipment information security protection system adapt to the special environment of information security, reliability, and confidentiality. Another purpose is to realize the particularity, advancement, practicability, and expansibility and of a certain type of engineering information security protection system.

1 Introduction

There is a general lack of top-level design and overall planning in the construction of the information security protection system (referred to as system) of some kind of engineering (referred to as engineering) in China. Specifically, there is not enough integration; the degree of automation is low; equipment compatibility and expandability is poor. Key domestic information security technology mostly uses foreign technology. There are great security risks in the information management of engineering and weapons. This paper is based on military and national standards, engineering and equipment use requirements. This paper focuses on network access security, desktop and centralized data management, data storage and backup, information exchange and input or output control, information security audit and other design. The design can ensure: a) officers and soldiers have access to the information system with a unique identity and permission; b) the completeness and practicality of the operational space for officers and soldiers; c)the confidentiality and completeness of information storage, disposal and transmission; d)the completeness of hardware, operating platform kernel, service and application software; e) the security of password use and storage; f)the protection capability of the engineering system. This paper can solve many bottleneck problems that restrict the combat effectiveness of engineering and weapons. It is of great significance to the promotion of the actual combat level. The analytical experience and results of this paper can be applied to the design and construction of similar engineering systems. It can also be used for reference by similar systems in other industries.

2 Design and analysis of the overall project of the engineering system

2.1 General scheme design principles

The system take security and confidentiality measures that combine technology and management. The principle of multiple-level depth defense or protection should be followed. We should adopt a variety of security means and design the information security system from various aspects and angles. It should have good scalability and maintainability. It shall be convenient to deploy, easy to use and centrally maintained. Services and applications should be scalable. The actual environmental needs should be met to the greatest extent. The particularity of engineering and equipment application should be fully considered.

2.2 Demand analysis of overall scheme design

Threats to engineering information mainly include natural disasters, malicious code, system problems, network access, physical access and so on. According to relevant national and military regulations and standards, the protection level of engineering information security should reach level 4. See table 1 for specific requirements.

[a]986031745@qq. Com; [b]12362441@qq. Com; [c]jessie_zhu2015@163. Com

The scheme design should integrate human, technology and operation means organically. The design of human-oriented means shall include organizational structure, personnel safety, safety awareness, safety training and other aspects. The design of technical means shall include identity authentication, network boundary or access control, security audit, host monitoring, terminal and information centralized control and so on. Operational means shall include system backup or disaster recovery, system monitoring, safety detection or evaluation and so on. The main content of the scheme design is shown in figure 1.

2.3 The design and analysis of the composition and function architecture of the overall scheme

Engineering system information security protection is a system engineering involving a wide range. A complete security system should be designed based on the overall security policy. Various technical measures for safety protection shall be adopted. Combined with a systematic safety management system, the overall protection of engineering and equipment information is achieved. The overall program design shall include safety management and safety technology. Security technology system design includes information security, equipment and facilities, network operation and other aspects. Safety management system design includes management organization, management technology, personnel management and management system and so on.

TABLE 1.ENGINEERING INFORMATION SECURITY PROTECTION REQUIREMENTS.

Protection type	***Functional requirements***
Network protection	Physical isolation from the Internet and public networks.
	Strictly control the unauthorized access of external network users.
	Discover network hidden trouble in time, fix security hole
	Effectively monitor and kill computer viruses
	Provide a unified network of virus detection and patch distribution services
Data protection	Real-time monitoring of network traffic data
	Encryption protects the transmission of confidential data
	Back up and protect important data regularly
Permission management	Real-time identification of a valid identity
	Implement network access control for computers and servers
	To implement identity authentication for networked computer users
	Assign user rights as needed
	Accurately record user and manager operations
	Effective audit access behavior and network application behavior

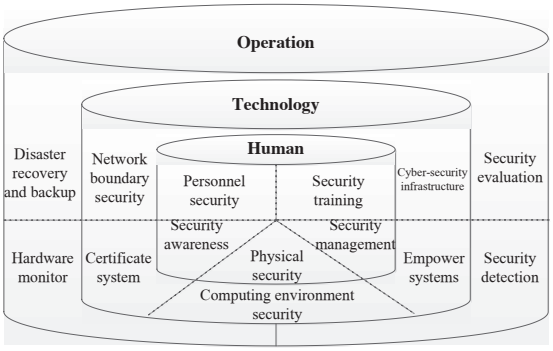

Figure 1. main contents of scheme design.

3 Design and analysis of information security technology protection system

The design mainly includes network access security, desktop and data centralized control, data storage and backup, information exchange and input or output control, information security audit and other parts. The information security technology architecture can be designed with reference to figure 2.

3.1 Design and analysis of network access security

Engineering information network should be designed as double core hot backup. The network core layer shall design two sets of relatively independent high-speed optical fiber links (Carry data such as management or control business applications and security monitoring). The security protection grade of engineering comprehensive information network is 4.The security protection grade of the military office network is 3.A boundary firewall and an encryption machine should be used for logical isolation between office network and engineering integrated information network. The servers and storage or backup devices of the engineering integrated information network access the backbone network through the switch (access end) on the server side and the server boundary firewall (access end).The engineering comprehensive information network server shall be divided into the comprehensive service data base area, the comprehensive business application service area, the out-of-band management area, the basic service area, the security product area, the data storage backup area, the security monitoring service area, the dynamic monitoring service area and other parts (divided according to the classification and business application).Access terminals are divided into different security domains and virtual VLAN at the aggregation layer (divided by business application or monitoring device type, department, etc.).Access control between

VLANs is accomplished through the terminal domain access boundary firewall. Each access terminal in the engineering system is bound to the network card MAC and network IP address of each device.

3.2 Design and analysis of network and application system security access control

The server devices and access terminals of the engineering integrated information network should be divided into different security domains and virtual VLANs (according to the classification of security and business applications).The server device and the access terminal access the boundary firewall through the server and the terminal domain, respectively to implement the authorized access to the IP layer node address and TCP layer port of the device. The non-secret application system (such as domain controller, DNS, etc.) operated by engineering integrated information network should adopt the authentication mode of user name and password, set certain password complexity and account locking policies. The secret application system should adopt the two-factor strong authentication mode (USB Key based on the PKI/CA certificate system), restrict the access of application system users to the background data (restricted by the security authentication gateway), and limit the access authorization of network user terminals (only authorized by the IP layer node address and TCP layer port of the application system).

3.3 Design and analysis of server, terminal and database security protection measures

1) The application system server shall be configured with the reinforcement system. Audit and manage the file operation control of the server host, registry operation control, process protection, file integrity detection, system operation log. Prevent unauthorized use of server host ports. The server should shut down unnecessary services; The server should start the process and protocol ports; Server system configuration and security policies should be optimized.

2) Application system server and access terminal should be configured with anti-computer virus Trojan system, patch automatic update system, etc. Patches and virus libraries should be updated regularly (automatically over the network).Regularly scans and fix vulnerabilities.

3) The secure access and audit of the engineering system server facilities (using out-of-band management domain and operation and maintenance audit system) should be protected.

4) The unified network domain security policy should be used to management and control the terminal (password, account locking, audit and other policies). The terminal host shall be configured with a secure login system. Achieve strong authentication system login (two factors based on USB Key and Pin code), terminal system locking, screen saver, user login operation audit and other functions.

5) Configure the security policy of binding domain users and domain terminal computers one by one; Configure terminal host security audit system, control port access, security audit, data and leakage prevention of the terminal host.

6) Database security protection design

Regularly update all applicable security patch installers (according to manufacturer's security bulletin);Improve database security through account and password, service configuration, auditing, managing extended stored procedures, transport protection configuration, service port and network connection configuration, database application system, etc. Divide the rights of the database system administrator (the highest authority administrator), for example, the secret keys and passwords are managed by two officers or soldiers, and the highest authority administrator does not do business work; Using specially developed applications to access the database; All applications do not directly operate manipulate the database; Each application should use a different account; Administrator account never develop applications; The database server is located in an independent security domain and a virtual VLAN. Only the relevant application servers are allowed to access the database server (controlled by firewalls, etc).

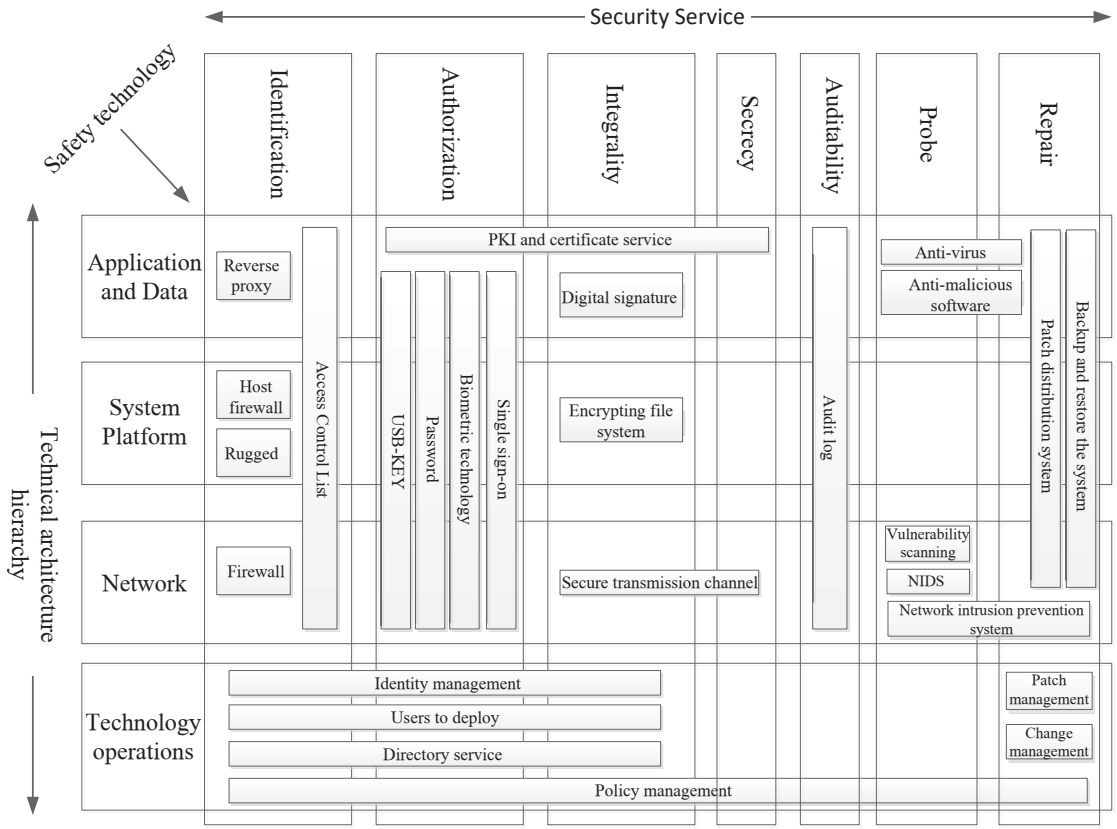

Figure 2. Information security technology architecture.

3.4 Design and analysis of desktop and data centralized security control

Structured data should be centrally stored in a unified data storage system behind the scenes (in block form through the SAN storage architecture set up on the server side). Unstructured data is stored centrally in a distributed data storage system or a unified back-end data storage system (in the form of Shared files through the NAS storage architecture set up by the server).Security NAS systems should be configured. The user data of the network access terminal is stored in the unified storage backup system. Through the software white list management system, unified management and centralized control of desktop applications and data of network users. A uniform system for data storage or backup and use should be designed. Operating platforms or systems and desktop applications or data for network access terminals shall be standardized and normalized.

3.5 Design and analysis of information exchange and input-output security control

Special information exchange points should be designed. Configuration information input and output port machine, information transfer machine. The port machine has the functions of input or output information content identification and detection, filtering and inspection, information hiding and detection, anti-entrapment, printing and burning information monitoring and audit, etc. (through the information input and output management platform, printing and burning monitoring and auditing platform).Mediators should deploy input or output filtering and checking, CD burning or auditing and anti-virus Trojans different from those on the network. Prevent the cross-use of information on mobile storage media and unauthorized output of information. The exchange of information in the integrated engineering information network shall be conducted through the secure NAS file system and other network application systems.

3.6 Design and analysis of information security audit

Information security audit is divided into network layer audit, system layer audit, application layer audit and data layer audit.

1) Network layer audit shall deploy network IDS system to intercept and analyze network data flow, listen and analyze (packet) network connection, network Shared files and resources, email, HTTP, FTP, Telnet, etc. And cooperate with network management software to audit and manage network.

2) The system layer audit shall deploy the terminal host monitoring and audit system on the access terminal; Deploy an operation and maintenance audit system on the server side. Control and audit the file system, registry, process, hardware interface and network activity of the terminal host, and issue security policy. Monitor and audit operational access to server systems.

3) Application layer and data layer audit shall cooperate with the operation and maintenance of the audit system. Monitor and audit user login, system authorization, data access and other operations at the application and data layers.

3.7 Design and analysis of data storage backup

Two data rooms should be configured in the project. Each computer room is equipped with a data storage and backup system. The storage and backup system uses array RAID redundancy technology to protect data. Allocate Hot Spare to replace when two disks are damaged. Use a dedicated disk (Log) to ensure file system security and stability.

The engineering system shall have a separate data storage and backup system. Develop full and incremental offline backup measures for different types of objects. A full backup is usually performed when the system changes significantly. Incremental backups are performed daily. It guarantees that in the worst-case (such as a low probability event where two storage system arrays damage three disks at the same time), only the day's new data is lost. Two storage and backup systems should have a secondary backup (DTOD, DTOT).Only in this way can the data security of information service and application system be guaranteed effectively. A single set of unified data storage capacity should be more than 40TB.The two data rooms in the project should be designed for high availability of network security resource pool, server resource pool, storage resource pool and database or application service resource pool (using virtualization, database cluster, application service middleware cluster and other technologies).Ensure high availability and failover of the system. A single set of unified data backup capacity should be over 90TB.It is equipped with a backup all-in-one machine to build a 1-layer disaster recovery platform (including backup management software and virtual band library).

Security system data volume is relatively large. According to national and military standards (1 year of data storage), the capacity of each data or storage system should be more than 3PB.Two separate distributed data storage systems should be configured.1 set of system is used for perimeter security system of engineering (placed in data room A).1 set of system for engineering security system (placed in data room B).At least 16 storage capacities (280TB distributed storage nodes) were designed for a single system. A single system can recover or reconstruct failed data of at least 4 physical nodes. The effective total capacity of a single system is above 3PB.

4 Conclusion

Similar engineering information management system needs are not the same. But the design philosophy and means are the same. The experience and results of the proposed scheme design are universal. Experience and results can be used in the design and construction of other similar projects, and can also be used for reference by relevant scholars.

References

[1] State Internet information Office. Network security and Informatization.Beijing, People's Education Press,2018..

[2] Lu Guiqing. Selected practical cases of engineering construction enterprise management informatization .Beijing, China Building Industry Press,2019.

[3] Xin Jiangyan. Enterprise informatization planning .Beijing, Tsinghua University Press,2017.

[4] Liu Xiguan.Enterprise informatization management practice .Beijing, Petroleum Industry Press,2013.

[5] Zuo Meiyun. Information system project management.Beijing , Electronic Industry Press,2014.