Network Security Protection Technology under the Background of Computing Big Data

Shanjie Chen*
Shandong CATV Network Co., Ltd Tai’an Branch, Tai’an, China

*Corresponding author: sdtacsj@126.com

Abstract. Based on the risk analysis of the network security of the radio and television critical information infrastructure, this paper introduces the evolution process of the network security protection architecture, and proposes the network security intelligent protection architecture. The article starts from the protection content and methods of physical security, network security, border security, server security, terminal security, application security, data security and backup and recovery, security management center and other technical aspects. Construction is explored. The thesis builds a reliable and stable broadcast technology center network information security system through the establishment of a network information security technology guarantee and a network information security management system.

Keywords: radio and television information; big data; network security protection; network information security technology

1. Introduction
At present, new-generation information technologies such as cloud computing, big data, artificial intelligence, and the Internet of Things continue to emerge and innovate, which promotes the transformation of radio and television enterprises from traditional broadcasting services to comprehensive digital, informatized, and customized services, and broadcasting and television networks to intelligent networks and wisdom. As the internal core system of a modern radio and television enterprise, the IT support system is related to corporate decision-making, business circulation, efficiency improvement, resource optimization and the normal operation of the company. However, network information security incidents such as information leakage, data tampering, denial of service, etc. are emerging in an endless stream [1]. At the same time, the country’s information security requirements for radio and television companies are constantly increasing. The information security of TV center business information systems should be divided into security domains and built-in depth. The defense system, hierarchical protection, etc., carry out a unified security strategy design to ensure the effectiveness of the overall security strategy. This article will refer to the industry standards for the security level protection of radio and television related information systems, and discuss the network security construction of radio and television information systems for the basic requirements of commonly used and widely-covered three-level information systems, in order to have
some enlightenment.

2. Security Technical Analysis

2.1 Basic network security

The basic network is the basic platform for carrying the TV center business information system. Starting from the concept of defense-in-depth, according to the degree of relevance of each information system to the broadcast business, the production and broadcast mixed information system, broadcast information system, etc. are directly related to the broadcast. The system is designed inside the network structure, and the production information system is designed outside the network structure, forming a deep network structure with increasing security requirements from the outside to the inside [2]. Divide the information systems with the same application or the same security requirements into the same security area to form an external area, exchange domain, integrated production domain, production and broadcast mixed domain, and broadcast domain (as shown in Figure 1).

![Fig.1 Schematic diagram of security domain division of TV center business information system](image)

The integrated production domain and the production and broadcast mixed domain exchange data with the office network, the Internet or other public networks through the data exchange area, and the broadcast domain exchanges data with the production and broadcast mixed domain through the broadcast boundary. In terms of network equipment configuration, in order to avoid network interruption due to the failure of the network equipment hardware itself, core switches and aggregation switches should be configured with redundancy and can be automatically switched. At the same time, the service processing capacity and network bandwidth of the network equipment should meet the service requirements. When remotely operating the device, it should be done through SNMPV3 and above or other secure network management protocols; in terms of access control, the network device should take measures such as ending the session, limiting the number of illegal logins, and automatically logging out after connection timeouts to handle login failures. Unnecessary services and ports on network equipment should be closed [3]. When accessing the device through the remote management address, it should be done through a secure communication protocol such as HTTPS, SSH, and the administrator login address of the network device should be restricted, and only the specified IP address or IP segment access is allowed. For qualified TV centers, the administrator's
identity authentication, authorization and audit can be realized through the operation and maintenance audit system.

2.2 Physical security
As an important information system for the national key industry, the third-level radio and television information system room has implemented high standards in the initial stage of construction, in terms of physical location selection, physical access control, anti-theft and anti-vandalism, lightning protection, fire prevention, and external power supply the vast majority of systems in other aspects meet the basic requirements. In recent years, with the vigorous advancement of the standardization of computer rooms, considerable experience has been accumulated in the design and layout of computer rooms and the selection of materials. There are relatively few network security incidents caused by physical security issues. Even so, physical security work should not be taken lightly, especially when external personnel enter the computer room to engage in related activities, the approval process must be completed and internal technical personnel must be accompanied.

2.3 Border security
The content that needs to be considered for border security, as the name suggests, refers to doing a good job of network security work on the border with external systems. Its main content includes boundary integrity check, intrusion prevention, and malicious code prevention. Boundary integrity inspection includes the inspection of unauthorized equipment or the behavior of privately connecting to the internal system, as well as the inspection of unauthorized equipment or the behavior of privately connecting to the external system, which is often referred to as illegal internal and external connection inspection [4]. Generally, the illegal inline behavior is realized by configuring the 802.1X protocol and authentication server on the network device, and the illegal outbound behavior is to prevent the host from logging in to the Internet by installing the internal network security management software. For network intrusion prevention, firewalls, IPS (Intrusion Prevention System), IDS (Intrusion Detection System) and other security devices are needed to control user access, and promptly warn and block illegal network intrusions. The prevention of network malicious code is mainly achieved through the anti-virus wall, and you can also choose a firewall with anti-malware function modules, such as UTM (Next Generation Firewall) and other equipment. It is worth noting that the network anti-malware code product needs to have a different virus database from the host anti-malware code software, and the third-level or above system is a product with a sales license of the Ministry of Public Security and a compulsory certification certificate for information security products when purchasing security equipment. Can be purchased, otherwise you need to bear certain legal responsibilities.

2.4 Application and data security
The user’s name and password requirements for server and application system for identity authentication are the same as those for network device identity authentication. When remotely managing servers and application systems, secure communication protocols such as HTTPS and SSH should be used. If operation and maintenance audit systems such as fortress machines are deployed, the operation and maintenance audit system can also be used for remote management identity authentication.

The server should close unnecessary services and ports and restrict the access rights of the default account or delete the default account, modify the default password of the account, delete redundant and expired accounts, and use the end of the session, limit the number of illegal logins and automatic logout after connection timeout Way to handle login failures. The server should not install applications and components that are not related to the production business. The operating system patch should be updated at least once every six months [5]. The server should also deploy anti-virus software. Before software update, patch update, and virus database update are performed on the server, the operating system should be updated at least once every six months. In the built test environment, test first, and then update after confirming that the update and upgrade content has no impact on the business.
application.

2.5 Terminal Security
For important business operations involving content approval, technical review, operation application and approval, in addition to user names and passwords, identity authentication should also pass security authentication mechanisms such as tokens, based on biometrics (such as fingerprints), and digital certificates, that is, two-factor authentication. Certification. At the same time, operating terminals that involve these important services should enable the operating system security audit function. The terminal security management system should be used to control the use of peripherals such as USB and optical drives, and only some port services of terminals that must be uploaded and downloaded through peripherals such as USB and optical drives should be reserved. Other terminals should be closed to peripheral interfaces such as USB and optical drives. For data uploaded and downloaded via USB, CD-ROM and other peripherals, first use two or more anti-virus software to perform strict virus detection, and then perform the upload and download operation. The update of the terminal's virus database and software version should be arranged during business idle hours to avoid affecting the business.

3. System security protection environment model
According to the technical requirements of the four-level broadcast system in various standards, combined with the security structure of the four-level broadcast system, the four-level broadcast system security protection environment model is shown in Figure 2.

Fig.2 A model diagram of the security protection environment for the broadcast system of a four-level TV station

Among them, the security goal of the four-level secure computing environment is to protect the terminals and servers of the computing environment, as well as the upper-level application security and data security, and to prevent intrusion events, detect and discover, emergency treatment, and audit trails [6]. The security goal of the four-level security zone boundary is to isolate and control the data and operation requirements transmitted through the security zone boundary, ensure the secure interconnection between the security zones and the safe access of legal terminals, and prevent users from illegal outreach and illegal operations. Eventually realize the prevention and prevention of intrusion events, detection and discovery, emergency treatment and auditing and tracing. The security goal of the four-level security communication network is to realize the operation safety protection of the communication network, the safety protection of data transmission and exchange, and the audit of
the communication network security event based on the safety of the communication network structure, and finally realize the prevention and detection of the communication network intrusion event., Emergency handling and audit tracking. The role of the security management center is to centrally manage and control the security mechanisms of the three parts of the secure computing environment, the secure area boundary, and the secure communication network. It is necessary to deploy corresponding terminal components in the secure computing environment, secure area boundary, and secure communication network.

4. Digital signature to realize the design of radio and television network security system

4.1 Overall system design
The task at this stage is to have the signer operate on this system, allocate a public-private key pair of a suitable strength algorithm, save it to a file and synchronize to the database. The model diagram at this stage is shown in Figure 3.

![Fig.3 Model diagram of application key and public key transmission stage](image)

4.2 Division of functional modules
As shown in Figure 4, the functional modules of the system are mainly: (1) Public and private key generation module; (2) Digest module; (3) Encryption module; (4) Decryption module; (5) Verification module. These five modules together form the key result, and pair the valid data from sending the public key to receiving the public key.
4.3 Encryption algorithm design
The RSA algorithm requires three parameters, $n, e_1, e_2$. Among them, $n$ is the product of two large prime numbers $p$ and $q$, and the binary representation of $n$ represents the number of bits occupied, which is the so-called key length. $e_1, e_2$ is a pair of related values, $e_1$ can be taken arbitrarily, but $e_1$ and $(p-1)*(q-1)$ are required to be relatively prime; then choose $e_2$, require $(e_2)$, and require $(e_1 * e_2) \mod (p-1)*(q-1)=1$. $(n, e_1)$ and $(n, e_2)$ are the key pair. The decryption algorithm is based on the following formula. The C implementation of RSA, the key generation flowchart is shown in Figure 5:

$$A = B \land e_2 \mod n$$
$$B = A \land e_1 \mod n$$

(1)
Faced with the generation and processing of public and private keys, both parties need to perform strict encryption algorithm processing, which is either controlled by the public key party or organized by the private key party. On the surface of the data, effective communication and coordination are required between the two. In the face of the data performance of the receiving parties, the key is the main factor of code control [7]. The application in the RSA algorithm should strengthen the penetration and use of this module. In the RSA algorithm, the receiver needs to further extend the data. The structure of the encryption algorithm is as follows. The first step is to receive the parameters from the user and determine how many keys the user needs to generate based on the parameters.

5. Experimental Design
The performance of the TV network information security precaution and Web data mining system shaped by experiments is tested. In order to test whether the method in this paper can accurately detect network information security, the experiment uses 700 broadcast and TV videos as training materials, and selects 2100 TV videos as actual test data. During the experiment, the test data was divided into three equally, and the unsafe information in the 700 articles in each was detected by the method in this paper. The test results of the method in this paper are shown in Table 1.

Table 1 Test results of the method in this paper

| Serial number | Total number of videos | The detection method of this article | actual results |
|---------------|------------------------|--------------------------------------|----------------|
|               |                        | Unsafe videos | Number of safe videos | Unsafe videos | Number of safe videos |
| 1             | 700                    | 92           | 585                     | 95            | 605                       |
| 2             | 700                    | 73           | 612                     | 76            | 624                       |
| 3             | 700                    | 84           | 594                     | 88            | 612                       |

Analysis of Table 1 shows that the unsafe information detected by the method in this paper is very close to the actual results, indicating that the method in this paper is effective. And it can be concluded from Table 2 that with the increase of time, the detection rate of the method in this paper increases,
and the rate of missed judgments and false judgments gradually decrease. It shows that with the passage of time, the performance of the network information security and Web data mining system designed in this paper is gradually enhanced, and it has high application value.

**Table 2 Performance of the method in this paper**

| Detection time/ms | Correct rate | Missing rate | Misjudgment rate |
|-------------------|--------------|--------------|------------------|
| 5                 | 0.976        | 0.222        | 0.0102           |
| 10                | 0.9802       | 0.2462       | 0.0001           |

The experiment evaluates the detection performance of Bayesian detection method and the method in this paper through recall and precision. The precision rate is the ratio of the number of detected unsafe information to the actual number of unsafe information, and the recall rate is the ratio of the number of detected unsafe information to the total network information. The method in this paper and the Bayesian detection method are used to detect the unsafe information in the experimental documents, and the results are shown in Table 3 and Table 4, respectively. Analyzing Table 3 and Table 4 are available, the recall and accuracy of the two methods are both high, and they can be used to monitor unsafe information in the network.

**Table 3 Bayesian detection method results table**

| Number of experiments | Recall rate | Precision |
|-----------------------|-------------|-----------|
| 1                     | 0.65        | 0.83      |
| 2                     | 0.88        | 0.71      |
| 3                     | 0.78        | 0.82      |
| average value         | 0.77        | 0.79      |

**Table 4 Results of the method in this paper**

| Number of experiments | Recall rate | Precision |
|-----------------------|-------------|-----------|
| 1                     | 0.92        | 0.86      |
| 2                     | 0.84        | 0.75      |
| 3                     | 0.88        | 0.92      |
| average value         | 0.88        | 0.84      |

6. Conclusion
We discussed some construction and protection contents of the technical level of the three-level system of the radio and television information system radio and television network security level protection. A safe, reliable, manageable and controllable network information system is constructed through various methods of security technology and security management. This will further optimize the work process, improve production efficiency and management level, greatly improve the operability, manageability, and superstability, and ultimately achieve the media strategy development goals of the entire world, and enhance the overall competitiveness of the media.

References
[1] Rodriguez, N. S. Negotiation of sexual identity in gay on-air talent on West Texas radio and television media. Journal of homosexuality, vol. 66, pp.896-913,July 2019.
[2] Catalan-Matamoros, D., Santamaria-Ochoa, C. D., & Peñafiel-Saiz, C. Message analyses about vaccines in the print press, television and radio: characteristics and gaps in previous research. Journal of Communication in Healthcare, vol. 12, pp. 86-101,February 2019.
[3] Hesmondhalgh, D., & Meier, L. M. What the digitalisation of music tells us about capitalism, culture and the power of the information technology sector. Information, Communication & Society, vol. 21, pp.1555-1570,November 2018.
[4] Xiong, C. B., Niu, Y. B., & Li, Z.An investigation of the dynamic characteristics of super high-rise
buildings using real-time kinematic–global navigation satellite system technology. Advances in Structural Engineering, vol. 21, pp. 783-792, May 2018.

[5] Martin-Shields, C. P. When information becomes action: drivers of individuals' trust in broadcast versus peer-to-peer information in disaster response. Disasters, vol. 43, pp. 612-633, March 2019.

[6] Al-Nassar, B. A. Y. The influence of service quality in information system success model as an antecedent of mobile learning in education organisations: Case study in Jordan. International Journal of Mobile Learning and Organisation, vol. 11, pp. 41-62, January 2017.

[7] Kiambi, D. The use of information communication and technology in advancement of African agriculture. African Journal of Agricultural Research, vol. 13, pp. 2025-2036, September 2018.