

Exploring Security Protection Design Concepts for Television Station Broadcasting Systems (Postprint)

Authors: Chen Lian

Date: 2023-10-08T00:00:00+00:00

Abstract

The broadcast system is the foundation for television stations to fulfill the aforementioned functions. Currently, issues of information loss and theft have emerged during the application of broadcast systems in television stations in China. To improve this situation and promote the healthy development of the entire industry, it is necessary to enhance the security protection level of broadcast systems. This paper analyzes and studies the design concepts for security protection of television station broadcast systems, starting from their composition.

Full Text

Exploring Design Approaches for Security Protection of TV Broadcasting Systems

Abstract: The broadcasting system serves as the foundation for television stations to fulfill their core functions. Currently, issues of information loss and theft have emerged in the application of TV broadcasting systems in China. To address these problems and promote healthy development across the industry, it is essential to enhance the security protection capabilities of broadcasting systems. This paper analyzes and investigates design approaches for security protection of TV broadcasting systems, beginning with an examination of system composition.

Keywords: TV station; broadcasting system; security protection design

CLC Number: G222

Document Code: A

Article ID: 1671-0134(2017)12-112-02

DOI: 10.19483/j.cnki.11-4653/n.2017.03.027

Author: Chen Lian

With the continuous development of internet and related technologies, the architecture of TV broadcasting systems has become increasingly complex. Due to the open nature of information dissemination, the information security of TV broadcasting systems faces certain threats. To ensure the normal operation and application of broadcasting systems, security protection design should be implemented to elevate the internal information security level.

1. Composition of TV Broadcasting Systems

TV broadcasting systems primarily consist of several integrated components, including upload network elements, broadcast business system elements, production business system elements, and media asset business system elements [1]. The security vulnerabilities of TV broadcasting systems mainly arise from information interactions among these multiple internal networks, as the constant exchange of data between different subsystems creates potential entry points for security threats.

2. Design Requirements for TV Broadcasting System Security Protection

To ensure that the designed broadcasting system meets the operational requirements of TV stations, the following principles should be adhered to during the design process.

2.1 Architectural Completeness Requirement

This requirement pertains to the system architecture of TV broadcasting systems. During actual design work, the security protection needs of every system component should be comprehensively considered. While reasonably satisfying the transmission requirements of different elements, the security level of internal files within the broadcasting system should be enhanced through a holistic approach that addresses potential vulnerabilities across all subsystems.

2.2 Data Integrity Requirement

This requirement addresses the data information within the broadcasting system. A program file contains substantial amounts of data, and the loss or corruption of some data may affect overall program quality [2]. Therefore, when designing security protection for TV broadcasting systems, the integrity of all data information within the system must be ensured throughout the entire production and transmission workflow.

3. Design Approaches for TV Broadcasting System Security Protection

This section analyzes and investigates the security protection design of TV broadcasting systems from multiple perspectives.

3.1 Security Protection Architecture Design

To enhance information security during transmission in TV broadcasting systems, the overall security protection architecture is designed as follows: the security gateway serves as an intermediate link in the broadcasting system information transmission, establishing effective connections between the security gateway and the TV station's business systems (production system, media asset system, and broadcast system). During actual transmission, external source materials are imported into the broadcasting system via external files. When the security gateway detection results indicate that the external file quality is acceptable (containing no abnormal information or security risks), the external file is permitted to enter the corresponding business system to provide file information support for the formal operation of the broadcasting system.

3.2 File Transmission Process

The file transmission forms in broadcasting systems based on security protection mainly include the following processes.

3.2.1 Secure Import Process for External Files into Broadcasting Systems In this information transmission process, external files need to be transmitted to the network through the TV broadcasting system site. At this point, the security gateway must perform its security protection functions. After passing security inspection, files are transmitted to the corresponding business system modules of the TV station based on task attributes [3]. This ensures that only verified external content enters the internal network.

3.2.2 Secure File Transmission and Delivery Process Between Media Asset System and Production System This file transmission process is critical to broadcasting systems. After TV station personnel produce a television program using the production system, the production system submits the program to the media asset business system's program repository. During this submission and transmission process, the security gateway evaluates the security status of the submitted file through security checks and ensures that no file damage or loss occurs during transmission. Additionally, when quality or content issues arise with program files, the media asset system needs to return the relevant program files to the production business subsystem of the broadcasting system. During this transmission process, the security gateway automatically performs security inspection and protection functions, allowing files from the media asset business system to be automatically transmitted to the production

business system after confirming the security status of the transmission object file is qualified.

3.2.3 Secure File Transmission Process Between Media Asset System and Broadcast System After relevant program files pass inspection in the media asset business system, they officially enter the transmission process to the broadcast business system. At this point, the security gateway utilizes its security inspection and protection functions to ensure secure transmission of program files between the media asset business system and the broadcast business system [4]. For viewers, the completion of this transmission process means they can watch the television programs produced by production personnel, satisfying their entertainment and leisure needs.

3.3 Security Gateway Characteristics

This section provides a detailed analysis of the security gateway characteristics that perform protection functions from multiple dimensions.

3.3.1 Performance Dimension At the performance level, security gateway characteristics mainly include the following: First, task priority transmission characteristic. In TV broadcasting systems, different transmission tasks (television program files) vary in viewing demand and processing content. To ensure normal system operation, TV station personnel can pre-sort security transmission tasks according to importance. During actual broadcasting system operation, the security gateway can leverage its task priority transmission characteristic to complete transmission of higher-priority television program files first, thereby indirectly improving the work efficiency of TV station personnel. Second, multi-task concurrent transmission characteristic. Based on previous experience with broadcasting system applications in TV stations, multiple file transmission requirements may arise simultaneously during particularly busy periods. The security gateway application provides an effective solution for concurrent transmission of multiple file types: TV stations can import multiple files awaiting transmission into the broadcasting system simultaneously [5]. The security gateway utilizes its multi-task concurrent transmission characteristic to transmit multiple file types into target business subsystems within the same time frame. Fundamentally, this characteristic can significantly enhance the timeliness of task transmission in TV stations, enabling broadcasting systems to better serve users.

3.3.2 Physical Dimension At the physical level, security gateway characteristics mainly include the following: First, six full gigabit network port characteristic. This characteristic provides an excellent port environment for file transmission between subsystems within TV broadcasting systems. Second, mechanical equipment characteristic. The advantage of this characteristic is that TV stations can deploy it in the central machine room, enabling it to provide

effective security protection functions for internal file transmission within the broadcasting system while maintaining physical security.

3.3.3 Functional Dimension At the functional level, security gateway characteristics mainly include the following: First, transmission file filtering characteristic. Before utilizing the security gateway to enhance broadcasting system security protection, multiple different types of file plugins should be pre-configured in the broadcasting system. During transmission, the security gateway uses its file filtering characteristic to make judgments: if the transmission object file finds a matching built-in file plugin during configuration selection, the transmission object file is permitted to transmit to the corresponding business system; if no matching plugin content is found for the transmission object file during configuration selection, the transmission object will be rejected by the security gateway. Second, transmission file identification characteristic. After the security gateway permits transmission object file transmission through its filtering characteristic, it continues to leverage its identification characteristic to determine whether the file format in the broadcasting system is consistent with the structure of the transmission object file. If identification results indicate differences between the two, the identified object transmission file will be rejected; if identification results indicate basic consistency in file format, the security gateway permits the transmission object file to transmit to the corresponding business subsystem. Fundamentally, this characteristic can effectively identify disguised files among numerous transmission object files [6], thereby ensuring the secure and stable operation of TV broadcasting systems. Third, transmission file virus checking characteristic. The virus checking module of the security gateway forms the basis for this characteristic. During actual broadcasting system operation, after the transmission object file passes the filtering and identification stages, the security gateway performs its virus checking function to examine the security status of the transmission object file. If checking results reveal viruses hidden in the file, the security gateway will not permit the file to transmit to the corresponding business subsystem of the broadcasting system. If checking results meet requirements, the transmission object file can be smoothly transmitted to the corresponding business subsystem in a secure state. Fourth, transmission file verification characteristic. After the virus checking stage, transmission files entering the broadcasting system require monitoring through the security gateway verification stage. Before permitting transmission files to the target path in the broadcasting system, the security gateway uses MD5 codes to conduct precise verification of both transmission files and original files [7]. The function of this characteristic is to ensure good consistency between original files and transmission files within the broadcasting system through verification. Fifth, transmission result feedback characteristic. During broadcasting system operation, when TV station personnel need to review transmission information for a particular file, they can obtain corresponding transmission information through the security gateway's Web interface.

4. Conclusion

To ensure information transmission security in TV broadcasting systems, security gateways can be integrated into TV broadcasting systems to enhance file transmission security levels. During actual operation of TV broadcasting systems, security gateways can utilize their physical, functional, and performance characteristics to identify problematic files containing viruses or format mismatches from among files awaiting transmission, thereby providing comprehensive protection for the entire broadcasting workflow.

References

- [1] Chen Jinming. Discussion on Design Approach for Security Protection of TV Broadcasting Systems [J]. Electronic World, 2016(12): 188-189.
- [2] Xiao Hang. Research on Boundary Protection Method for TV Broadcast System Based on Security Domain Division [J]. Science and Technology Communication, 2016(16): 111, 136.
- [3] Chen Yu. Design and Practice of P2 Card Security Protection Management System for Beijing TV Station HD News Network [J]. Modern TV Technology, 2011(07): 42-45.
- [4] Gong Minghao, Wang Xiaoyan, Liang Jinchun. Research on Boundary Protection Method for TV Broadcast System Based on Security Domain Division [A]. China Association of News Technical Workers. Proceedings of Outstanding Papers from the 2015 “News Technology Papers” of China Association of News Technical Workers [C]. China Association of News Technical Workers, 2015: 5.
- [5] Wang Xiaoyan, Liang Jinchun, Yao Yingying, Wang Yanan. Research on Boundary Protection Method for TV Broadcast System Based on Security Domain Division [J]. Cable TV Technology, 2015(03): 97-99, 102.
- [6] Cao Jiucheng, Yan Haidong. Network System Security Design Analysis—Regarding Yancheng TV Station Satellite Program Recording System [J]. Audio-Visual World (Broadcasting and Television Technology), 2010(02): 47-50.
- [7] Zhou Wei. Design and Implementation of CCTV Network Information Security Platform Construction Planning and Key Technologies [D]. Tianjin University, 2014.

Note: Figure translations are in progress. See original paper for figures.

Source: ChinaXiv — Machine translation. Verify with original.