Postprint of Network Security Strategy for Radio and Television Monitoring Network

Authors: Wei Jinhao

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

Abstract

The rapid development of informatization and networking in the broadcast industry has transformed broadcast monitoring from previously scattered, single manual operations into modern approaches that are networked, intelligent, and systematic. The establishment of monitoring networks has catalyzed qualitative transformations in monitoring work, enhancing information feedback rates, enriching monitoring data content, expanding monitoring business varieties, broadening monitoring geographical coverage, and substantially improving the overall monitoring capabilities of the broadcast industry. However, with the continuous expansion of network scale, the complexity and risk of monitoring networks have gradually intensified, while business expansion imposes increasingly stringent requirements on network performance. How to adopt advanced technological solutions to ensure monitoring network stability constitutes a major challenge currently faced.

Full Text

Cybersecurity Strategies for Broadcasting and Television Monitoring Networks

ChinaXiv Cooperative Journal

Abstract

The rapid informatization and networking of the broadcasting and television industry has transformed monitoring from fragmented, manual operations into modern approaches that are networked, intelligent, and systematic. The establishment of monitoring networks has fundamentally changed monitoring work, improving information feedback speed, enriching monitoring data content, expanding monitoring service categories, and broadening monitoring geographical coverage, thereby significantly enhancing the overall monitoring capabilities of

the broadcasting industry. However, as network scale continues to expand, the complexity and risk of monitoring networks gradually increase, while business expansion imposes higher demands on network performance. How to adopt advanced technological solutions to ensure monitoring network stability represents a major challenge currently faced.

Keywords: Broadcasting and television industry; monitoring network; network security; strategy analysis

Classification Code: TN915.08
Document Code: A
Article ID: 1671-0134(2019)07-114-03
DOI: 10.19483/j.cnki.11-4653/n.2019.07.037

Author: Wei Jinhao

Broadcasting and television monitoring networks constitute a fundamental and core task within the broadcasting industry, with monitoring quality closely linked to the public' s spiritual and cultural life. As domestic broadcasting programs at all levels continue to increase and broadcasting networks continuously expand, the service scope of monitoring networks gradually broadens, making monitoring processes increasingly complex and task volumes larger, which poses significant risks to stable network operation. Moreover, the rapid proliferation of various broadcasting derivative projects also imposes higher requirements on network quality. Consequently, broadcasting security represents a factor requiring high-level attention and preventive vigilance. For broadcasting and television monitoring networks, this is also a challenging task that must not be neglected in terms of quality, security, and monitoring capabilities.

1. Broadcasting and Television Monitoring Network System Analysis

The monitoring system is based on computer network platforms, gigabit Ethernet systems, dynamic routing systems, and link redundancy systems, forming an integrated information transmission network that combines video, voice, and data. Given the characteristics of monitoring networks—large information transmission volumes, high timeliness requirements, and high demands for information security, stability, and uniformity—the following requirements must be considered during the overall network design phase:

(1) Implement a robust firewall system and develop comprehensive security processing plans to meet confidentiality requirements, supporting multiple security functions including AAA, ACL, IPSEC, NAT, routing verification, CHAP, PAP, CA, MD5, DES, logging, and various other capabilities.

(2) The network's physical architecture, logical architecture, and address space must be hierarchical and modular, with standardized technologies and products, and possess sustainability to facilitate network construction and

expansion; as the network evolves, it should be continuously extendable while fully protecting existing resources.

(3) The system must exhibit strong fault tolerance, high damage prevention capabilities, and robust stability, where a single point of failure within the network will not cause a local area network to lose connection with the entire network, and multiple anomalies will not partition the entire network into several disconnected segments.

(4) Meet the requirements for multi-service operations, providing a high-performance service network capable of serving images, voice, and data.

(5) Communication protocols and interfaces must comply with international standards.

(6) Network planning should be based on current requirements and foreseeable growth, avoiding emphasis on hollow technical sophistication and preventing excessive expenditure from pursuing high-end and latest technologies.

(7) Possess high transmission bandwidth and maintain strong throughput performance and efficiency under high-load conditions with minimal latency.

2. Security Issues in Monitoring Network Systems

Currently, domestic broadcasting and television monitoring network systems face significant security issues, specifically manifested as follows:

2.1 Complex System Layout Affects Security

The most prominent characteristic of China' s broadcasting industry is its correlation with vast national territory—the industry' s coverage is extremely broad, encompassing the vast majority of China' s land area, including some uninhabited regions. Correspondingly, the monitoring network platform continues to expand, resulting in geographical dispersion, cumbersome diversity in communication methods, and distributed node layouts within China' s broadcasting monitoring system. Precisely because of these characteristics, implementing comprehensive, efficient, and truly secure monitoring becomes extremely difficult.

Due to inconsistencies in facilities and technologies among various domestic broadcasting entities, some well-developed large provincial and municipal television stations have already deployed broadcasting facilities that exceed central-level capabilities. Furthermore, each broadcasting station can adopt different and multiple coexisting communication modes for information transmission and dissemination. Since each information transmission method and monitoring approach differs, this complexity poses significant threats to monitoring system security. The most common challenge of distribution is that distributed monitoring systems require corresponding layouts, but distribution is not the

ultimate goal—the final objective is to achieve real-time centralized management and control. While distribution across a vast region is already difficult, obtaining real-time centralized control becomes even more challenging.

2.2 Inherent Security Issues in IP Networks

Broadcasting monitoring systems worldwide, including domestic systems, are all TCP/IP protocol-based architectures similar to Internet structures, alongside monitoring network platforms relying on wireless and analog signals. Although TCP/IP networks have a relatively long history, their reliance on the openness, connectivity, accessibility, and detectability of the TCP/IP protocol makes them highly vulnerable to attacks.

2.3 Incomplete Management Systems

Despite the rapid development of broadcasting and television monitoring networks and their massive expansion in scale, current efforts still lack centralized security standards, comprehensive management systems, and legal provisions regarding system establishment, secure network platform operation, and data confidentiality. System management involves not only control over computers, network facilities, and system software, but also governance of overall data resources and standardized, scientific management of data assets. Only by establishing scientific security management systems can security countermeasures at the physical layer, application layer, and other levels be truly effective.

2.4 Hacker Intrusion into Computer Systems

Hackers represent a critical factor threatening network security. Hackers within computer systems utilize their specialized computer knowledge to destroy computer network platforms, constituting the primary perpetrators of computer system crimes. They employ self-written or other virus tools to detect vulnerabilities within networks before launching attacks. Various hacker activities profoundly threaten computer system security. Compared with standalone environments, network platforms feature high communication capabilities, enabling rapid virus transmission while simultaneously increasing the difficulty of virus detection. From a physical perspective, computer system security remains relatively fragile. As illustrated in the broadcasting system network structure diagram (see Figure 1 [Figure 1: see original paper]), the broadcasting system comprises several network processes including content production, signal transmission, transmission configuration, and customer reception. Similar to issues encountered in communications, computer networks involve widely distributed facilities that no individual or department can monitor comprehensively at all times. Any equipment installed in unsecured locations, including communication optical cables, cables, LANs, telephone lines, and remote networks, may suffer damage, potentially causing computer system paralysis and hindering normal information service transmission. Hazards in daily operations include: reduced stable operational efficiency of computer and network systems, damage

to computer operating platforms and customer information, damage to computer hardware platforms, and theft of critical data.

3. Security Countermeasures for Broadcasting and Television Monitoring Networks

Cybersecurity countermeasures for broadcasting and television monitoring networks must comprehensively consider both technical and management measures. From a technical perspective, due to the complexity of adopted systems, monotonous security countermeasures cannot meet the intricate demands of application systems. Therefore, multiple security countermeasures are required, and much like various application systems operating within the same network, network security also necessitates a centralized, comprehensive processing plan that establishes a hierarchical security system architecture.

3.1 Operating Platform Security Countermeasures

Security vulnerabilities in operating platforms largely result from inadequate system management, such as poorly configured passwords without regular updates, improper file permission settings, and inappropriate server configurations. It is essential to establish a comprehensive operating platform security upgrade system to promptly download and install patches.

3.2 Backup Strategies

To ensure the secure and reliable operation of monitoring networks, dual hot standby plans can be implemented for critical LAN platform hardware within the security network. Hardware such as application servers, database servers, file servers, switches, and firewalls can operate in dual-machine parallel mode with load balancing, ensuring that when any point fails, the system can intelligently switch to hot standby hardware without affecting stable system operation. However, this solution requires substantial investment. Under budget constraints, hot backup plans can still be adopted, but they necessitate regular manual backups and maintenance testing to reduce resolution time when failures occur.

3.3 Network Resource Design Countermeasures

Before establishing a monitoring network, network resources must be uniformly planned, with scientific IP addressing schemes and network topology designs developed. Various resources should be centrally encoded to create a centralized information dictionary. Practice demonstrates that scientific, centralized network planning offers significant advantages for network maintenance and secure operation, helping ensure long-term reliability during continuous network expansion and enabling persistent resolution of technical faults.

3.4 Equipment Security Configuration Methods

For core network equipment such as switches and routers, scientific configuration management methods must be established, including disabling non-essential services, implementing strong passwords, enhancing equipment access authentication and authorization, updating BIOS, employing access control list permissions, and restricting packet types.

3.5 Anti-Virus Countermeasures

Viruses constitute a common hidden danger in network security, continuously threatening all networks due to their rapid transmission and strong destructive capabilities. From an architectural perspective, monitoring network platforms feature widespread node distribution, necessitating multi-angle, multi-level anti-virus platforms.[1] By adopting unified management and multi-level protection methods, anti-virus software can be deployed at graded levels across each network within the monitoring network, with the core network implementing unified virus monitoring for subordinate platforms and performing regular updates. During the management control phase, centralized anti-virus countermeasures should be formulated and adopted, which can both reduce administrator workload and ensure that every computer, server, and client throughout the network maintains consistent and robust anti-virus protection capabilities.

3.6 Network Security Countermeasures

First, firewall platforms. Due to layout constraints, monitoring networks typically consist of multiple security domains requiring firewalls to block core ports, implement access management at each security boundary, and log all traffic. Firewalls enable separation and access control between networks at various system levels, provide security protection for publicly accessible service equipment, enable secure authentication and ACLs for remote clients, and facilitate traffic control, management, and intrusion prevention for dedicated line information. The core of effective firewall implementation lies in the allocation and control of its security policies. For monitoring networks with only a single LAN platform, firewalls are installed at network entry points to monitor network communications; for distributed monitoring platforms with multiple LANs, firewalls can be deployed in conjunction with network grading settings for unified control.

Second, LDS platforms. LDS platforms represent a new type of network security system that can supplement firewall limitations, effectively handle attacks originating from within the network, and provide robust network protection.[2] For hierarchical control platforms, LDS platforms can be installed behind each LAN firewall in a distributed layout, with each region conducting information analysis on network traffic. When abnormal behavior occurs, evidence is recorded and alerts are sent to network controllers, displayed at both local sub-centers and the main monitoring center for unified network behavior analysis and centralized implementation of scientific prevention measures.

Finally, vulnerability scanning. Security vulnerability scanning platforms represent the most scientific systems currently available, with security assessment technologies capable of periodically and aperiodically scanning monitoring networks and various platforms to provide security administrators with scientific system vulnerability information, enabling timely understanding of existing vulnerabilities and implementation of appropriate remediation measures.

Additionally, network management countermeasures. Network security protection systems are established by people, applied by people, and controlled by people. Since the initiators of network attacks are also human, the key to network security lies in people. Network security management must be strengthened, as relying solely on simple technical tools is far from sufficient to achieve security objectives. Evaluating the security of an internal network requires examining not only its technical measures but also the integrity of the various methodologies employed by the network.

3.7 Information Transmission Security Countermeasures

Monitoring networks are wide area networks without dedicated communication infrastructure, primarily relying on broadcasting optical cables and telecommunications lines for communication. Information transmission across wide area networks must employ encryption methods.[3] Due to diversified transmission forms, encryption methods vary under different circumstances. For instance, using VPN systems and dynamic encryption systems requires establishing different information transmission countermeasures based on various communication modes and information security levels.

3.8 System Security Countermeasures

All security products serve only specific aspects of security and possess certain limitations. Networks represent diverse, complex, and dynamic platforms; no single security product or technology can meet all network security requirements. Firewall platforms cannot prevent internal attacks or behaviors disguised as legitimate requests, while intrusion monitoring and vulnerability scanning frequently generate false positives and false negatives.[4] Moreover, simply stacking numerous security facilities cannot enhance network platform security levels. Network security constitutes a multi-stage integration; for example, when IDS platforms detect malicious network behavior, they can coordinate with firewalls and critical protection systems, and when anti-virus platforms identify new viruses, they must immediately update the virus attack database of IDS platforms to improve their operational efficiency. Only through effective linkage and mutual complementarity among all network security components can network security be ensured.[5] Furthermore, as business systems themselves are in developmental stages, security strategies must evolve alongside system adjustments to maintain scientific validity.

3.9 Identity Authentication Strategies

First, password-based identity authentication mode. Traditional authentication technologies employ password-based methods. This approach is relatively simple and represents a scientifically effective solution for closed, small-scale platforms. However, when selecting passwords, customers typically choose names and birthdates, making such passwords extremely vulnerable to cracking and thereby creating significant security threats.

Second, physical token-based authentication forms. This method is implemented through customers' specific physical possessions, including smart cards and USB keys. Smart cards can encrypt hardware systems, offering high security levels. Smart card-based authentication combines two factors—what the customer knows and what the customer possesses—by storing customer data within the physical token and pre-selecting certain random information stored in the Authentication Server (AS). When customers access system resources, after entering their ID and password, the system first verifies the smart card' s validity, then uses the smart card to authenticate customer identity. If the customer identity is legitimate, the random information stored in the smart card is subsequently transmitted to the AS for deeper authentication.

Finally, one-time password authentication methods. One-time passwords involve using identity codes and certain unpredictable factors as input parameters for cryptographic algorithms. Through algorithmic transformation, a changed result is obtained and used as the customer's login password. The authentication service device performs the same calculation and compares it with the customer' s login password; if legitimate, login is permitted. Such one-time passwords are non-repetitive and continuously changing. Additionally, customers need not memorize them, as each password can be used only once and is designed to refuse repeated use. Currently, one-time password authentication methods are primarily implemented through three approaches: (1) Lamport scheme. Also known as hash chain mode, this plan is relatively easy to implement and requires no special hardware support. However, its security is based on one-way hash functions and should be avoided in distributed network conditions. (2) Time synchronization mode. Under this mode, each customer possesses a time-synchronization token. The core of this approach is ensuring clock synchronization between the authentication server and the token. (3) Challenge-response mode. Under this mode, all customers maintain challenge-response tokens containing seed keys and encryption algorithms. When customers access the system, a challenge message is randomly generated by the server and transmitted to the customer. The customer inputs the received information into the token, which calculates the corresponding response information using its internal encryption algorithm and seed key. The customer transmits this response information to the server, which calculates the relevant response information and compares it with the uploaded information for verification.

In summary, with the advancement of computers and related technologies, mon-

itoring system security must maintain a dynamic operational concept through regular inspection and evaluation, continuous system upgrades and patch installation, tracking of latest security risks, system transformation aligned with business progress, technological innovation, adjustment to higher-quality products, or continuous expansion and extension of security performance through topological compensation to ensure stable system operation. Network control is critically important in network construction and maintenance; only by establishing and implementing robust security control standards to ensure prevention before problems occur can monitoring network security work be guaranteed.

References

[1] Jia Wancai. Wireless Broadcasting and Television Monitoring Network and Security Strategy[J]. Heilongjiang Science and Technology Information, 2014(03):37.
[2] Hu Maogui. Research on Network Security of Anhui Broadcasting and Television Monitoring Network[J]. Network Security Technology and Application, 2013(08):126-127.
[3] Li Tao. Research on Network Security of Broadcasting and Television Monitoring Network[J]. China New Communications, 2013, 15(04):33.
[4] Chen Yufeng. Wireless Broadcasting and Television Monitoring Network and Security Strategy[J]. Heilongjiang Science and Technology Information, 2011(24):109.
[5] Li Jingen. Research on Network Security of Broadcasting and Television Monitoring Network[J]. Science and Technology Innovation Herald, 2011(24):237.

(Author affiliation: Xining City Broadcasting and Television Monitoring Center)

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