Advances in Computer, Signals and Systems (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2025.090217
ISSN 2371-8838 Vol. 9 Num. 2

Exploration of Computer Network Information and Network Security and Its Protection Strategy

Yan Jingtao

Xijing University, Xi'an, Shaanxi, China
jingtaoyan0301@163.com

Keywords: Computer Networks; Information Security; Network Security Protection

Abstract: With the evolution of the digital tide, the methods of social operation are changing; computerized network information has become the lifeblood of modern society. However, the industrialization of cyber-attacks, rampant ransomware, and constant data leakage incidents demonstrate how fragile the security defenses are. This article focuses on the core elements of confidentiality, integrity, and availability of network information, and is in turn, concerned with a myriad of threats, including malicious attacks, internal leakage, and physical encroachment. Research confirms that no single technology can handle dynamically shifting risks. It is imperative to assemble a multi-layer defense strategy that demonstrates intelligent filtering characteristics of firewalls, the real-time response capability of intrusion detection systems, and the forward-looking deployment and strategy encapsulated by quantum encryption. More importantly, technology must be synchronized with management - the absence of a corporate security culture is more catastrophic than a system failing. A resilient line of defense in the offense-and-defense game can only be developed by reconstructing the security operation and maintenance processes, augmenting the management control of behavioral patterns, and establishing a flexible activation mechanism.

1. Introduction

Mission essential activities - financial transactions, dispatching of energy, medical diagnoses - each rely on reliability of the network. The double-edged sword of reliability manifest itself in some pretty grave ways: ransomware has shut down hospital emergency systems; industrial control devices have been taken over, halting production; and private data of citizens is traded on the black market. Cyber security has gone from an IT issue, to a national security strategic issue. Traditional mindsets of security protection are obviously limited. They have focused too much externally while ignoring internal human error; they have pursued a stacking technology posture while ignoring proper closed-loop management. This paper cuts through the instrumental lens of understanding and asserts that security protection is simply a continuous risk management process. By unpacking the evolution of cyber-attack technologies and ignoring new variables such as the internet of things and weaponized artificial intelligence, this paper presents activities for a protection paradigm that clarifies a blend of technology and management are required for a theoretical basis to create a trustable cyber space.

2. Basic concepts of computer network information and network security

2.1. Definition and Characteristics of Computer Network Information

Information in computer networks is the means of production of the digital age. Specifically, the information consists of the electronic data generated, transmitted and stored in computer systems connected through communication devices and transmission media. This information reflects an inherent dynamic quality in an open architecture, constantly changing form as it flows through each layer of the OSI model - to the current pulses at the physical layer, readable semantics at application layer and the value density of the information increasing at exponential levels. The substantive facets focus on three dimensions: first is the spatio - temporal penetrability. For example, transnational financial transaction instruction can travel half - way around the globe in 67 milliseconds, breaking the physical barriers of conventional information dissemination. Second, is the multi - state correlation [1]. The readings of one single sensor, via big - data correlation analysis, may reveal the operating condition of a country's entire infrastructure, and the reconstitution of apparently fragmented data can deliver global perspectives through intelligent recombination. Third is the dual - sided vulnerability. Cloud - based medical images not only provide accurate diagnostic support for patients but also become high - value targets for ransomware encryption and extortion. This inherent contradiction requires the protection system to adapt to both the tool and weapon attributes of information simultaneously. Understanding the essence of continuous fission of information during its circulation is the logical starting point for building an effective defense.

2.2. Main Objectives of Network Security

The core mission of cyber security lies in maintaining the reliable operation of the digital ecosystem, and its goal system is built around the information life cycle. Confidentiality, as the fundamental defense line, requires that sensitive data be visible only to authorized entities. The encrypted storage and transmission isolation measures for medical records embody this principle, preventing unauthorized extraction of patients' privacy during shared diagnosis and treatment. Integrity assurance focuses on the trustworthy state of data. The blockchain - style verification mechanism adopted by financial transaction systems rejects any abnormal tampering after the decimal point, ensuring that changes in account balances are absolutely consistent with the actual flow of funds. The goal of availability is often underestimated but is crucial for business survival. The redundant channel design and traffic shaping strategies of industrial control networks ensure that critical instructions can still reach production - line controllers during peak DDoS attacks. These goals have dynamic priority characteristics. Government systems may prioritize integrity to maintain public credibility, while cloud - gaming platforms focus more on millisecond - level availability response. Security architects must understand the restrictive relationships among the three. Excessive encryption may slow down the retrieval of emergency medical images, and one - sided pursuit of service continuity may overlook the risk of data leakage, the ideal protection mode needs to flexibly balance the tensions among the three according to business scenarios [2].

3. Major security threats to computer networks

3.1. Types of Network Attacks

Contemporary cyber attacks are trending towards highly specialized division of labor. Malware threats have transitioned from single - machine viruses to a "ransomware - as - a - service" business model. By renting cloud - based control platforms, hackers can target attacks against medical

institutions encryption hardware, hijacking the image scheduling system in emergency rooms until paid ransom in the form of Bitcoin. Intrusion - type attacks utilize software supply chain vulnerabilities to gain entry. A multinational manufacturing enterprise suffered a three - month infiltration of the program running backdoor for its production - line control system through unpatched open - source components. Service - disruption attacks are trending towards coordinated attacks with IoT botnets. Smart home devices are compromised to act as traffic amplifiers to attack e - commerce platform gateways, which result in attacks against backend servers with millions of forged requests per second to exhaust session resources. Credential - stealing attacks are yielding improvements through methodology types that include social engineering. In the banking sector, the number of cases involving forged voice instructions from executives to mislead financial staff into permitting large - scale transfers continues to rise. As attack patterns integrate artificial intelligence technology for adaptive evolution, they will continue to pose foundational problems for conventional detection methodologies relying on signature - matching.

3.2. Insider Threats

The covert nature of internal threats makes them the most difficult risk category to defend against in an enterprise's security system. Employees with legitimate access rights may cause systematic damage due to the temptation of personal gain or operational negligence. When a R & D staff member copied unencrypted design drawings to a personal cloud drive, it led to the circulation of new - type engine patent data on the black market. An operation and maintenance engineer accidentally exposed the database monitoring port to the public network, allowing attackers to inject malicious scripts and tamper with the content of millions of electronic invoices. A sales supervisor deleted the encryption key of the customer relationship management system before leaving the company, making it impossible to recover the enterprise's three - year market expansion records. The failure of the access control mechanism exacerbates the risk. A finance intern exported sensitive salary information using a leftover domain administrator account. These incidents reveal that internal protection needs to go beyond the traditional boundary - defense mindset, continuously audit the operation trajectories of high - privilege accounts, and establish a dynamic trust model that combines minimum access control with behavioral baseline analysis [3].

3.3. Physical security threats

Physical - level security vulnerabilities are often overlooked by digital protection systems. Attackers directly accessing hardware devices may trigger a chain - reaction security collapse. During an unmonitored maintenance window in a data center, malicious individuals can implant counterfeit solid - state drives into the storage array. After three months of operation, these components activate a firmware - level backdoor, gradually encrypting financial transaction logs and bypassing all network - layer detections. The risk of electromagnetic radiation leakage is equally fatal. A special receiving device placed in an office next to a government affairs computer room can capture scattered screen signals, restoring the content of classified documents without touching the network perimeter. Environmental factors pose non - intentional threats. A malfunction in the temperature control system of a substation in a coastal city causes the server room temperature to rise to a critical point. Multiple core switches shut down due to over - temperature protection, forcing the customs clearance platform to suspend services for eight hours. These cases indicate that physical protection requires the establishment of a hardware supply - chain auditing mechanism, the implementation of thermodynamic monitoring and electromagnetic shielding projects for critical facilities, and the inclusion of physical access rights in the authentication scope of the zero - trust architecture.

4. Computer network information and network security protection technology

4.1. Firewall technology

As the cornerstone of network boundary defense, firewalls establish controlled channels between trusted and untrusted domains through a policy - driven traffic filtering mechanism. Modern firewalls have evolved into intelligent gateways with deep application - layer detection capabilities. After deploying a next - generation firewall in the image archiving system of a top - tier hospital, it successfully blocked an attempt by ransomware disguised as DICOM protocol data packets to penetrate. The device identifies abnormal payload characteristics by parsing the unique grammatical structure of medical image transmission. The traditional port management and control model faces the risk of ineffectiveness in the cloud - native environment. The lack of effective isolation of east - west traffic within the container cluster led to a supply - chain attack on an e - commerce platform. Attackers used the unmonitored communication between Pods to move laterally to the database nodes. Current firewall technology is integrating machine - learning algorithms to build an adaptive policy model, dynamically adjusting the intensity of access control rules for financial transaction systems during peak business hours, while maintaining the response speed of the payment gateway and intercepting credit - card brute - force attacks. The coordinated policy management of physical firewalls and virtualized instances has become a key support for the hybrid - cloud security architecture [4].

4.2. Intrusion Detection and Prevention System (IDS/IPS)

In the practice of building a dynamic network security defense line, Intrusion Detection and Prevention Systems (IDS/IPS) play a crucial role in identifying and immediately responding to malicious activities. The core value of such technical solutions lies in their ability to continuously monitor network traffic or host behavior. By using a sophisticated abnormal behavior analysis engine and a mechanism that compares with a vast signature feature library, they can acutely detect potential attack signs or known malicious operation patterns. Different from traditional Intrusion Detection Systems (IDS) that only provide passive alarm functions, Intrusion Prevention Systems (IPS) with active defense capabilities go a step further. After confirming a threat, they can automatically execute pre - set strategies, resolutely block malicious data packets or session connections, and intercept attacks before they cause substantial damage. They are usually deployed at key boundary nodes or core areas of the network, such as behind firewalls or in front of important server clusters, forming an indispensable real - time response layer in the in - depth defense architecture. An efficient intrusion detection and prevention system not only significantly shortens the threat exposure window period, but the detailed security event logs it generates also provide a solid basis for subsequent forensic analysis and security policy optimization, substantially enhancing the overall security resilience of the network environment.

4.3. Encryption Technology

As the cornerstone for safeguarding information confidentiality and integrity, encryption technology plays an irreplaceable and central role in combating the threats of network eavesdropping and tampering. Its basic operating principle relies on complex mathematical algorithms, which transform original readable plaintext information into incomprehensible ciphertext. Only authorized parties with specific keys can perform the reverse operation to restore the original content, thus forming an effective protective layer during data transmission or static storage. The modern encryption system mainly consists of two major types: symmetric encryption

and asymmetric encryption. Symmetric encryption uses a single key to achieve an efficient encryption and decryption process, making it suitable for scenarios requiring rapid processing of massive amounts of data. Asymmetric encryption, on the other hand, relies on the pairing mechanism of public keys and private keys, ingeniously solving the traditional problem of secure key distribution and laying a solid foundation for digital signatures and identity authentication. As an important extension of encryption technology, hash algorithms provide a reliable means to verify whether information has been unauthorizedly modified during transmission by generating unique fixed - length data fingerprints. These technologies are deeply integrated and applied in multiple aspects of daily network interactions. For example, the HTTPS protocol that ensures the security of web browsing relies on SSL/TLS encryption channels. Virtual Private Networks (VPNs) protect remote access data through encrypted tunnels, and email and file storage systems widely use encryption methods to prevent the leakage of sensitive content. It is this invisible barrier built by encryption technology that enables the effective maintenance of information privacy and authenticity even in an environment where network paths may be snooped on, making it a core supporting element for building a trustworthy digital space [5].

4.4. Authentication and access control technology

In the crucial process of establishing a trustworthy access mechanism in cyberspace, authentication and access control technologies serve as the first gatekeeper for digital resources. Their core mission is to accurately verify user identities and strictly limit the scope of their operation permissions. The authentication process is like a rigorous identity check, requiring users to provide credentials such as passwords, dynamic tokens, biometric features, or digital certificates. The system verifies their authenticity by comparing pre - stored information or invoking authoritative authentication services. Among them, multi - factor authentication combines multiple verification elements, significantly increasing the difficulty of impersonation. Once the identity is confirmed, the access control mechanism takes effect immediately. It divides users' operation permissions for system functions, data files, or network services in a refined manner according to preset security policies. For example, the role - based access control model links permissions to job responsibilities, while the attribute - based access control model makes dynamic decisions based on user characteristics and the environment. This refined management permeates the deep - seated architecture of daily network applications. Employees need to go through an identity verification process when logging into the corporate intranet. Database management systems display different data views according to user roles. Cloud service platforms strictly limit tenants' configuration permissions for their virtual resources. It is the coordinated operation of authentication and access control technologies that effectively blocks unauthorized access by non - authorized users and restricts the behavior boundaries of legitimate users. Fundamentally, it reduces the risk of data leakage caused by internal misoperations and external penetrations, and forms an indispensable part of the network security protection system.

5. Network Security Management Strategy

Building an effective network security management strategy is the fundamental guarantee for an organization to cope with the dynamic threat environment. Its core lies in establishing a continuous governance framework that integrates strategic planning, technical controls, and personnel collaboration. This strategy begins with the clear commitment and resource investment from senior management, deeply embedding security goals into the business development blueprint and forming a top - down responsibility transmission mechanism. The specific implementation process covers multi - dimensional collaborative actions: conducting periodic risk assessments to identify key

assets and potential threats, and formulating differentiated protection priorities accordingly; designing a multi - layer defense technical solution covering the physical environment, network boundaries, terminal devices, and application systems, and standardizing configuration through the establishment of a unified security baseline; establishing a mandatory security awareness training system to enable employees in different positions to understand their security responsibilities and operating norms; and improving the support framework that includes incident response plans, disaster recovery processes, and compliance audit systems. The vitality of the strategy depends on a continuous monitoring and optimization mechanism. The security team needs to regularly verify the effectiveness of control measures, analyze the root causes of security incidents, and adjust the strategy details based on audit results, forming a closed - loop management of "assessment - improvement - verification". This systematic management method transforms discrete security practices into organizational resilience, providing institutional support for the confidentiality, integrity, and availability of information assets while balancing business efficiency and security requirements.

6. Conclusion

Cybersecurity is a perpetual offensive-defensive struggle. Research suggests that even current encryption algorithms will be vulnerable to quantum computing, and AI- and data-based adaptive attacks will eventually overwhelm rule-based defenses, signaling the inherent temporal limits of technical protections. True sustainability in the security ecosystem must disengage from technical reliance and discover a path toward three important areas. First, embed a security culture into the DNA of an organization. Employees adhering to behavioral norms are potentially significantly more effective at blocking phishing attacks than firewall policy enforcement. Second, create a dynamic "monitoring-response-tracing-reinforcement" closed-loop and utilize red-team vs. blue-team exercises to discover and reveal blind spots in defense. Third, encourage cross-border threat intelligence exchanges and global governance pooling. The tipping variable in cybersecurity in the future is not simply another iteration of technology, but for the in-depth integration of human nature insights and institutional function. Only when the mentality surrounding security transitions from a passive approach to one of active immunity can we possibly defend our core values in this wave of digital civilization.

References

[1] Sun J. Computer network security technology and prevention strategy analysis[J]. Procedia Computer Science, 2022, 208: 570-576.

[2] Liu L. Discussion and practice of computer network information and network security protection strategy[C]//2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE). IEEE, 2020: 1810-1813.

[3] Xue R. Exploration of Information Security Protection Strategies for Computer Networks in the Era of Big Data[J]. International Journal of Advance in Applied Science Research, 2025, 4(1): 6-11.

[4] Liu J. Exploration of Factors Influencing Computer Network Information Security and Prevention Strategies in Colleges and Universities[C]//2024 5th International Conference on Education, Knowledge and Information Management (ICEKIM 2024). Atlantis Press, 2024: 595-606.

[5] Xue L, Yang J, Fan W. Protection Strategy Exploration for the Computer Network Information Security in the Big Data Age[C]//2016 2nd Workshop on Advanced Research and Technology in Industry Applications (WARTIA-16). Atlantis Press, 2016: 81-85.