GEORGE BROWN PRESS
JOURNALS, BOOKS & PROCEEDINGS

Journal of Computer, Signal, and System Research

Article

Design and Implementation of Computer Network Security Monitoring System

Yihong Zou [1,*]

[1] Amazon Data Services, Inc, Intent Driven Network, Cupertino, California, 95014, United States
* Correspondence: Yihong Zou, Amazon Data Services, Inc, Intent Driven Network, Cupertino, California, 95014, United States

Abstract: With the increasing complexity of computer network security issues, traditional security protection methods are unable to meet the needs of dynamic network environments. In response to this challenge, this article has developed an innovative computer network security monitoring system. The system adopts a modular architecture and has key functions such as real-time monitoring, threat analysis, and automatic response. It mainly consists of network data collection unit, data preprocessing and storage module, threat detection, and security event response mechanism, effectively detecting and processing various potential risks. The system integrates multi-faceted security visualization technology, presenting clear security event analysis results and log review functions to users. The experimental results show that the system exhibits outstanding advantages in data traffic monitoring, attack tracing, risk assessment, and security policy implementation, providing a solid technical foundation for addressing security challenges in complex network environments.

Keywords: network security; monitoring system; threat detection; data collection; visualization

1. Introduction

In the information society, computer network security has become a core issue that urgently needs to be addressed. Traditional security protection strategies often focus on static protection measures, which are inadequate in the face of changing and complex network attacks. Building a network security monitoring system that can dynamically respond in real-time, operate efficiently, and have intelligent analysis capabilities can significantly enhance the efficiency of discovering potential threats and improve the speed of handling security incidents. This article will explore the key characteristics, system architecture, and modular implementation of network security monitoring systems, providing comprehensive security solutions for network security.

Received: 02 May 2025
Revised: 06 May 2025
Accepted: 29 May 2025
Published: 31 May 2025

2. Characteristics of Computer Network Security Monitoring System

2.1. Real time and Efficiency

The real-time and efficient performance of computer network security monitoring systems is a significant feature, mainly reflected in data processing, threat response, and system construction. This system captures real-time data streams in the network through its fast data collection module, including core elements such as communication protocol types, sending and receiving addresses, and packet size. At the same time, it uses deep packet inspection (DPI) technology to conduct in-depth analysis of packets, achieving a response time measured in milliseconds. Faced with massive data traffic, the system adopts a decentralized structure to distribute data to different nodes for parallel processing, thereby improving computational efficiency and reducing latency [1]. The real-time monitoring mechanism also has the ability to dynamically update the policy library,

which can quickly identify and detect newly emerging attack methods, and prevent security risks caused by policy update delays. This system integrates an efficient memory caching scheme, temporarily storing data traffic in fast cache to alleviate the pressure of hard disk I/O. To maintain efficient performance, the system adopts intelligent resource allocation algorithms and adjusts resource allocation strategies in real-time based on network traffic fluctuations, ensuring stable operation during peak traffic periods.

2.2. Intelligence and Automation

The core of intelligence and automation for building a computer network security monitoring system lies in data analysis, threat detection, and strategy implementation. This system integrates advanced artificial intelligence technology and uses deep learning and machine learning to model historical data streams, in order to extract typical features of attack behavior. During real-time data stream monitoring, the system is able to dynamically compare these features in order to accurately identify diverse attack methods. The intelligent log analysis module can automatically detect abnormal activities during the operation of the system, replacing the traditional reliance on manual analysis with efficient automated processing. The automated strategy development module generates protective measures to address the current threat environment based on real-time monitoring results and preset rules, such as implementing traffic control, isolating infected nodes, and other response strategies. The system has automated response capabilities and can work in conjunction with network devices such as firewalls and routers to quickly implement security policies [2].

3. Architecture Design of Computer Network Security Monitoring System

3.1. Network Data Collection

Network data collection constitutes the core component of computer network security monitoring systems, mainly used to intercept data packets circulating in the network in real time and provide the necessary initial information for subsequent data analysis. The system utilizes deep packet inspection (DPI) technology to conduct detailed analysis of information flow and obtain key information, including source address, destination address, port number, communication protocol category, and traffic attributes [3]. The data collection module also needs to be compatible with multiple protocols and multi-level data capture, covering a wide range of protocol types from the data link layer to the application layer, to ensure the integrity and accuracy of data. In the process of data collection, the system reduces the probability of packet loss through efficient caching strategies and stores network data according to time segments, thereby improving the efficiency of data collection. The total flow of collected data Dt at time t can be expressed as:

$$D_t = \sum_{i=1}^{n} (p_i \cdot s_i) \quad (1)$$

Among them, p_i represents the priority of the i-th packet, s_i is the size of the packet, and n is the total number of packets in the time slice. To ensure the security and integrity of information, the system adopts encryption methods to protect critical information during the data collection stage. This module is capable of implementing a multi node distributed architecture, which can maintain efficient operation even under complex network conditions, providing accurate data foundation for subsequent risk analysis work.

3.2. Data Preprocessing and Storage

In the network security monitoring system, data preprocessing and storage play a crucial role. Its main task is to purify, screen, and extract features from the collected data, and then store these processed data in a high-performance database for subsequent analysis and application [4]. The initial data often contains redundant, incomplete, or abnormal data. The system uses data cleaning algorithms to remove useless components, and classifies and organizes the data based on communication protocols, time stamps, and

other factors to optimize the efficiency of storage procedures and data analysis. The preprocessing module uses feature extraction algorithms to transform complex raw data into easily analyzable feature vectors F, whose calculation formula is:

$$F = \frac{\sum_{j=1}^{m} w_j \cdot x_j}{\sqrt{\sum_{j=1}^{m} (x_j)^2}} \tag{2}$$

Among them, w_j represents the feature weight, x_j represents the j-th feature value of the original data, m is the number of feature items, and the sum of squares of the denominators in the formula is used to normalize the feature vectors, ensuring the consistency of the data's magnitude. The data is stored in a distributed storage system designed to meet the needs of high-frequency access and agile retrieval. The system utilizes a specific time-series database to process time-series data, enabling rapid identification of security events at critical time points during analysis. In order to further improve access efficiency, the system has adopted index optimization technology, effectively reducing the time required for queries, enhancing the overall performance of the system, and providing guarantees for long-term stable operation.

3.3. Threat Analysis and Detection

In the network security monitoring system, threat analysis and detection play a crucial role, with the main task of conducting in-depth analysis and threat detection on the collected and initially processed network information. The system adopts a multi-level detection mechanism, which involves traffic anomaly detection, network protocol behavior analysis, and feature comparison detection. In terms of traffic anomaly detection, the system identifies behavior patterns that exceed the norm by studying various statistical indicators of network traffic. For example, using clustering algorithms to classify traffic characteristics into two categories: normal and abnormal. In terms of protocol behavior analysis, the focus is on reviewing whether the protocol operation is compliant, in order to discover possible abuse or covert attack behavior. Feature comparison detection matches data packet characteristics against a pre-set attack feature library to quickly identify known threats. The system also integrates machine learning algorithms, which can dynamically grasp newly emerging attack features through model training. The architecture also includes a real-time updated threat intelligence unit that can connect to external databases to obtain the latest attack identifiers and threat information. Figure 1 shows the complete workflow of the threat analysis and detection module from traffic anomaly detection to threat report generation and feedback, clearly reflecting the logical relationship and execution sequence of each functional module [5].

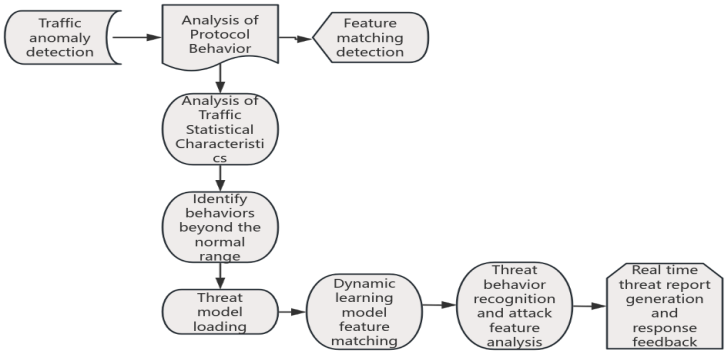

Figure 1. Threat Analysis and Detection Process.

3.4. Security Incident Response and Control

The security incident response and control module is an important component of the computer network security monitoring system, and its architecture design needs to meet the requirements of efficiency, automation, and real-time processing. The system consists

of four core components, including event activation, strategy implementation, resource allocation, and effectiveness feedback. In the event activation stage, the system activates the corresponding response mechanism according to the pre-set rules based on the risk assessment data output by the threat analysis module. The strategy implementation part introduces a pre-set security policy library, which flexibly adopts measures such as isolation, traffic blocking, or access restriction, based on the urgency of the event, the nature of the threat, and the scope of impact. The resource allocation unit is responsible for the function of allocating system resources, ensuring the smooth execution of emergency measures even in high load environments, such as using distributed frameworks to allocate computing tasks, achieving task splitting and synchronous processing. The feedback mechanism tracks the status and effectiveness of the response process, records relevant data in the logging system, and feeds back to the threat analysis module to optimize future detection strategies. The system architecture has hierarchical management functions, including local response and global control, which can quickly prevent the spread of security incidents and continuously optimize its security protection and operational efficiency through feedback mechanisms.

4. Modular Implementation of Computer Network Security Monitoring System

4.1. Network Traffic Monitoring and Log Collection

When building a network traffic monitoring and log collection system, refine it into four functional modules. This includes traffic capture, data filtering, feature extraction, and log storage, forming a closed data processing system. The traffic capture module uses deep packet inspection technology to perform real-time monitoring of network traffic during transmission, and obtains core elements such as traffic scale, communication protocol category, and time stamps from it. The data filtering module adopts a list filtering and rule comparison mechanism to exclude irrelevant and abnormal data, ensuring that only traffic information related to analysis is left. The feature extraction module uses aggregation analysis methods to abstract traffic information into traffic pattern features, such as transmission direction and time delay features, and then forms a feature set for in-depth analysis. The log storage module adopts an efficient distributed architecture, which associates and stores processed feature data with raw data, and achieves fast retrieval and tracking through index optimization technology. The time trend of features can be described by the following formula:

$$R_t = \max（T_{\text{end}} - T_{\text{start}}) \tag{3}$$

Among them, R_t represents the maximum time interval within a certain time window, while T_{start} and T_{end} represent the start and end times of the data stream, respectively. This formula is effective in capturing abnormal activity characteristics on the timeline, especially in dealing with sudden traffic situations, demonstrating its significant application value. Its modular structure enhances the processing performance of the entire system and also contributes solid technological strength to traffic supervision work.

4.2. Attack Traceability and Risk Assessment

The attack tracing and risk assessment module is crucial in network security monitoring systems. The design of this unit adopts a modular architecture, covering data collection module, log analysis module, path tracking module, and risk assessment module. The data collection module utilizes deep packet inspection (DPI) technology to monitor network data streams in real-time, collecting key data such as communication protocol types, source and destination addresses, and transmission times, providing complete raw data for subsequent processing modules. The log processing module deeply analyzes traffic logs and security event logs, filters out suspicious behavior time points, access paths, and abnormal attributes. The path tracing module integrates network structure and routing information, and uses a reverse tracing algorithm to accurately identify the attack

source location. The risk assessment module is based on analyzing data, quantifying risks from multiple perspectives such as impact amplitude, threat level, and target importance, and preparing an assessment report. The module also has an automated response function, which can activate security policies based on evaluation results, such as isolating specific nodes or restricting specific data traffic. The collaborative effect between these modules significantly enhances the accuracy and efficiency of tracking and evaluation, enabling the system to dynamically respond to threats. Table 1 shows the specific functional division and technical implementation of the attack tracing and risk assessment module.

Table 1. Modular Implementation of Attack Traceability and Risk Assessment.

Module Name	Function Description	implementation technique
Data Acquisition Module	Real time monitoring of network traffic, recording key information such as protocol type, source and destination addresses, transmission time, etc	Deep packet inspection (DPI) and traffic mirroring technology
Log analysis module	Analyze logs, extract the time and access path of attack behavior	Pattern matching algorithm, abnormal feature extraction
Path tracking module	Analyze the attack traffic path and locate the network location of the attack source	Network routing analysis and reverse path derivation algorithm
Risk assessment module	Quantify risk levels, generate assessment reports and strategic recommendations	Threat classification model and impact range analysis model
Automated response module	Trigger dynamic security policies based on evaluation results, such as isolating attack nodes or limiting traffic	Dynamic strategy triggering mechanism, device linkage interface
Collaboration module	Coordinate data exchange and task allocation between modules to ensure efficient traceability and evaluation processes	Distributed architecture design, multi-threaded task scheduling

4.3. Automated Security Policy Generation and Execution

The automated security policy generation and execution module is a key module for achieving dynamic response in network security monitoring systems. Its modular design is divided into three main parts: policy generation, optimization, and execution. In the strategy development phase, this module constructs real-time security protection strategies that are suitable for current risks based on threat intelligence, rule libraries, and intelligent algorithms, such as data flow isolation, permission control, and node blocking measures. As for the strategy adjustment process, the module will monitor network resource allocation, workload status, and business needs in real time, and fine tune established strategies, such as optimizing blocking scope, setting processing priorities and operation sequences, aiming to achieve the best balance between risk control and business continuity. The strategy execution phase ensures that optimized strategies can be quickly deployed to various nodes in the network, such as firewalls, routers, and intrusion detection systems, and real-time tracking of the effectiveness of strategy implementation is carried out. This module also adopts a closed-loop feedback mechanism, which dynamically adjusts the strategy model by collecting traffic dynamics and behavioral characteristics during the execution process, in order to enhance the accuracy and execution efficiency of future strategy formulation. The calculation formula for the execution priority of automation strategy is as follows:

$$P = \frac{\alpha \cdot L}{T + \beta \cdot R} \tag{4}$$

Among them, P is the priority of the policy, L is the threat level score, T is the time required for policy execution, R is resource consumption, and α and β are weight fac-

tors that measure the weight of threat level and resource impact, respectively. This formula ensures rapid response and resource optimization of the strategy by comprehensively evaluating threat level, time consumption, and resource load.

4.4. Multidimensional Security Visualization and Log Audit

When building a computer network security monitoring system, its functions are divided into four basic modules: data collection, threat analysis, automated response, and visualization. The data collection module uses deep packet inspection technology to instantly intercept network traffic, and provides detailed analysis of key elements such as communication protocols, timestamps, and address information to ensure that the system obtains a comprehensive data foundation. The threat analysis module integrates machine intelligence and pattern recognition technology to conduct in-depth analysis of collected data, in order to identify and form specific threat reports. Based on the analysis results, the automatic response module automatically formulates security policies and cooperates with network firewalls, routers, and other devices to implement emergency measures such as isolation, current limiting, or blocking. The visualization module displays data and analysis results to the manager through interfaces such as dashboard, network topology diagram, and timeline, in order to comprehensively monitor the operating status of the system. The interaction between these modules relies on a distributed architecture to efficiently complete parallel processing, enable threat identification, and facilitate security response in complex network environments.

5. Conclusion

The design and implementation of a computer network security monitoring system is an important guarantee for addressing security threats in complex network environments. This system adopts a modular architecture, integrating functions such as data collection, threat analysis, automated security policy generation and execution, multi-dimensional security visualization, etc., to build a complete process from risk identification to response. The close coordination of various components within the system enhances the timeliness and accuracy of threat handling, as well as the ability to respond quickly to new types of threats. The integration of automated security policy modules and multidimensional visualization technology greatly enhances the effectiveness of network security protection. In the future, with the continuous changes in security threats, the upgrading and improvement of the system's intelligence and self-adjustment capabilities are indispensable to ensure that it can face more severe security challenges and lay a solid foundation for creating a secure and reliable network environment.

References

1. L. Tan, K. Yu, F. Ming, X. Cheng, and G. Srivastava, "Secure and resilient artificial intelligence of things: a HoneyNet approach for threat detection and situational awareness," *IEEE Consum. Electron. Mag.*, vol. 11, no. 3, pp. 69–78, May 2021, doi: 10.1109/MCE.2021.3081874.
2. G. Engelen, V. Rimmer, and W. Joosen, "Troubleshooting an intrusion detection dataset: the CICIDS2017 case study," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2021, pp. 7–12, doi: 10.1109/SPW53761.2021.00009.
3. T. M. Booij, I. Chiscop, E. Meeuwissen, N. Moustafa, and F. T. Den Hartog, "ToN_IoT: The role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion data sets," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 485–496, Jan. 2022, doi: 10.1109/JIOT.2021.3085194.
4. T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Comput. Electr. Eng.*, vol. 99, p. 107810, Jan. 2022, doi: 10.1016/j.compeleceng.2022.107810.
5. K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, and A. K. Bashir et al., "Securing critical infrastructures: Deep-learning-based threat detection in IIoT," *IEEE Commun. Mag.*, vol. 59, no. 10, pp. 76–82, Oct. 2021, doi: 10.1109/MCOM.101.2001126.