Intelligent Computer Security Monitoring Information Network Analysis

Yong Sun* and Haiwen Wang*
School of Economics and Trade, Jilin Engineering Normal University, Changchun 130000, China
*Corresponding author Email: bwsn050401@163.com, *markxy@sohu.com

Abstract. At present, network information security monitoring still has problems such as poor processing capability, insufficient depth and breadth of detection, joint processing problems, and slow time. Based on this, the paper collects and stores web logs based on Web Service and Oracle10g database, and exchanges, communicates and encrypts data through SOAP and SSL; realizes data analysis service using J2EE platform; and realizes cross-platform display using Flex. The hardware and software implementation and test results show that the proposed system can quickly respond to various network security attacks, improve the work efficiency and work level of network information security monitoring, and reduce the risk and cost of network operation.

1. Introduction
At present, with the continuous development of computer and technology, computers have become an indispensable auxiliary tool in all walks of life [1-2]. Due to the openness and sharing of computer networks, most network monitoring cannot provide comprehensive and flexible intelligent monitoring of computer security [3]. In this case, how to effectively monitor the computer for security intelligence becomes a problem to be solved in this field. The effective computer security intelligent monitoring method can firstly design the hardware of the computer security intelligent monitoring system, and carry out the computer security intelligent monitoring based on the hardware construction result [4]. It is an effective way to solve the above problems, which has attracted the attention of many experts and scholars in this field. Since computer security intelligent monitoring is of great significance to the development of computers, it has become the focus of researchers in computer network security intelligent monitoring technology. Great concern. In this paper, the architecture of distributed network security event monitoring system is proposed for the security management of large-scale networks. The system designed and implemented can detect security events such as system vulnerability scanning, SQL injection, remote control Trojans and DDoS attacks in large-scale networks, to meet the needs of network security management. After the trial operation, the system found that the security intelligence monitoring requirements were met.
2. Current status of intelligent computer in security monitoring information network technology

Intelligent computer security monitoring plays a key role in the further development of computer technology. For this reason, it is a key part of the research that must be paid to by researchers involved in intelligent computer security monitoring information network technology. After experiencing long-term related research, scholars in the industry have achieved certain achievements in the computer security intelligent monitoring methods.

Some researchers have established a "Computer Service" based on "Web Service" and proposed an intelligent computer security monitoring method [5]. By using the DFNMS system, a security check device is set at the entrance of the computer information network and the exit of the computer information network, respectively, to filter the inflow of the data flow into the computer network, and the flow of the information out of the computer network, by analyzing the data streams. Find information that is unsafe or risky, and implement intelligent security monitoring of the computer by taking such a method of checking for missing traps. Under this method, for confidential content data, the submission can be blocked immediately, which is beneficial to reduce the probability of active disclosure. However, this method requires a security inspection device at the entrance of the computer information network and the exit of the computer information network, which is relatively high in cost, and requires regular maintenance inspection, which increases the cost of maintenance inspection and wastes time.

![Figure 1. Computer Security Monitoring System Based on Web Service.](image1)

Some researchers have adopted a new method of intelligent computer security monitoring while using "GPRS".

![Figure 2. GPRS-based computer security monitoring system.](image2)
With the aid of a remote network monitoring system, the computer is monitored for security. At the same time, the monitoring code is used to accurately mark the remaining security in the computer network, and the terminal communication link of the computer is utilized. Providing unsafe information at a lower security level to the manager, who then remediates the computer. After using this method, intelligent security monitoring can be applied to the computer to obtain the unsafe information remaining in the computer network at any time. However, this method can only implement remote monitoring, but it cannot play the role of risk assessment, so it is easy to cause the safety monitoring results of intelligent computers to produce large or small differences [6].

3. Research on Intelligent Computer Security Monitoring Information Network Technology

3.1. Computer network security intelligent monitoring system design

Computer network security is easily affected by various network security factors. To achieve computer security and intelligent monitoring, it is necessary to classify computer security factors, which is an important part of computer security intelligent monitoring, which is convenient for intelligent monitoring of computer security. 1) Computer network configuration; 2) Computer network own system; 3) Computer network virus. Therefore, the intelligent monitoring of computer security is mainly for the analysis of these three aspects of security risks, which is conducive to more thorough prevention and handling of computer security issues. A computer security intelligent monitoring platform is designed for the security factors of computer security intelligent monitoring. The platform refines the monitoring of various parts of the computer. The specific platform design is shown in Figure 3.

![Figure 3. Computer security intelligent monitoring platform.](image)

3.2. System Process

As shown in FIG. 3, the process flow of the system is introduced by taking the traffic flowing through the router R1 as an example. 1) Router R1 generates a stream record and outputs the record to the stream detection server. Stream records conform to IPFIX format, and streams are identified by quintuple (SrcIP, SrcPort, DestIP, DescPort, Protocol). 2) The flow detection server uses the flow feature-based detection method to detect the traffic, divide the traffic into normal traffic and security event traffic, and send the classification result to the system center. 3) The system center analyzes the detection results according to the monitoring strategy in the security event policy library. There are three situations: the traffic is normal: no control is required, and the system displays the detection result. The test result reaches the control standard: an alert is issued or the configuration server is notified to control the specific traffic, and the configuration server accepts the notification and executes. Deep packet inspection is required: notify the configuration server to mirror specific traffic
on R1. 4) The configuration server issues a related mirror configuration command to R1. 5) R1 executes the mirroring command to mirror the corresponding traffic through the mirroring link. 6) The load detection server captures these data messages and determines them for analysis by the deep packet inspection method. 7) Display the detection result, issue an early warning to the security event or notify the configuration server to implement control. 8) The server sends a configuration command to configure the corresponding edge router.

3.3. System Implementation

The system uses the XML language to describe the characteristics of the packet, using five types of elements: logic, operators, constants, functions, and macros, each of which contains multiple symbols. The following is a partial description of the remote-control Trojan feature.

```xml
<Bot Signature>
  <S1 type="Logic" symbol="&amp; &amp;"/>
  <S2 type="Logic" symbol="&amp; &amp;">
    <S4 type="Logic" symbol="&amp; &amp;">
      <Equal type="Logic" symbol="==">
        <Make_Int type="Func" symbol="MakeInt">
          <Get_Payload type="Func" symbol="GetPayload">
            <Const_Parameter type="Const" symbol="0"/>
          </Get_Payload>
        </Make_Int>
        <Substraction type="Arith" symbol="-">
          <Get_Payload_Len type="Func" symbol="GetPayloadLen"/>
          <Const type="Const" symbol="4"/>
        </Substraction>
        <Equal>
          <Equal_Greater type="Logic" symbol="\geq">
            <Const type="Const" symbol="78"/>
            <Get_Payload type="Func" symbol="GetPayload">
              <Const type="Const" symbol="4"/>
            </Get_Payload>
          </Equal_Greater>
        </Equal>
      </Equal_Greater>
    </S4>
  </S2>
</Bot Signature>
```

3.4. Monitoring Module and Risk Security Evaluation Module

Based on the hardware design of the 3.3 computer security intelligent monitoring system, based on the computer security intelligent monitoring distortion attenuation suppression method, the distortion of the computer security intelligent monitoring is effectively suppressed, and the computer security is obtained according to the distortion suppression result of the computer security intelligent monitoring. Intelligent monitoring information state transition probability matrix and computer security intelligent monitoring information state transition confusion matrix, using computer security intelligent monitoring beam control method to control computer security intelligent monitoring information beam shape, generally using amplitude beam control, measured according to time period Z. The computer security intelligence monitoring information sensitive features are segmented in the sequence:
\[ w_{Br} = \begin{cases} \frac{2n}{M-1} & 0 \leq n \leq \frac{1}{2}(M-1) \\ 2 - \frac{2n}{M-1} & \frac{1}{2}(M-1) \leq n \leq (M-1) \end{cases} \]  

(1)

Among them: \( w_{Br} \) represents the similarity matrix of tampering computer security intelligence monitoring information, and \( \frac{2n}{M-1} \) represents the computer security intelligence monitoring information beam control amplitude. The mathematical expectation value of the computer security intelligence monitoring information packet loss rate predicted by the computer security intelligent monitoring information distortion attenuation suppression method is:

\[ w_{ith}(n) = \left( 0.55 - 0.47 \cos \frac{2\pi n}{M-1} \right) R_M(n) = 0.6 \left( 1 - \cos \frac{2\pi n}{M-1} \right) R_M(n) \]  

(2)

Among them: \( w_{ith}(n) \) represents the mathematical expectation value of computer security intelligence monitoring information packet loss rate, and \( R_M(n) \) represents computer security intelligence monitoring information distortion attenuation suppression prediction value. Finally, using the MAX3491DSP system to obtain real-time intelligent monitoring of remote security information, data and signals, thus achieving remote security monitoring of computers. Assume that there are \( m \) indicators in the indicator system layer of the overall operation of the computer security and intelligent monitoring environment, and invite \( n \) experts to vote and comment on these computer security intelligence monitoring indicators, and then the concentration of expert opinions on each computer security intelligence monitoring indicator and the dispersion is counted. Among them, the computer security intelligence monitoring information concentration of expert opinions is:

\[ E_i = \frac{1}{n} \sum_{j=1}^{n} a_j \quad (j = 1, 2, \ldots, m) \]  

(3)

Expert advice on computer security intelligence monitoring information dispersion can be used standard deviation:

\[ \sigma_i = \sqrt{\frac{1}{n-1} \sum_{j=1}^{n} (a_j - E_i)^2} \quad (i = 1, 2, \ldots, m) \]  

(4)

Among them: \( E_i \) is the concentration of expert opinions; \( \sigma_i \) is the dispersion of expert opinions; \( a_j \) is the evaluation value of the \( j \)th expert. According to the characteristics of computer security intelligence monitoring information, based on \( E_i \leq 3 \) and \( \sigma_i \leq 0.63 \), the evaluation indicators of the overall operation of the computer network security environment are screened, and the evaluation index system of computer security intelligence monitoring the overall operation of the network environment is established. The computer security intelligent monitoring integrated risk security assessment is realized. The system has good operational effect, versatility and scalability in the computer security intelligent monitoring network. It is a good evaluation index for the overall operation of the computer security intelligent monitoring network environment system.
4. Operation result analysis
The system achieves better results in a certain university system. Figure 4 shows the real-time monitoring interface of the system's network traffic. It graphically shows the number of sessions for real-time communication, the distribution of various protocol traffic, and the application of Top10.

![Real-time monitoring interface](image)

**Figure 4.** Real-time monitoring interface.

5. Conclusion
When the current method is used to monitor the computer security intelligence, the non-security factor weights in the computer security intelligent monitoring cannot be obtained, so there are problems such as low efficiency and large monitoring error. Collect and store network logs based on Web Service and Oracle10g database, and exchange, communicate and encrypt data through SOAP and SSL; use J2EE platform to realize data analysis service; use Flex to realize cross-platform display. The simulation experiment proves that the proposed method can comprehensively and accurately monitor the computer security intelligently, which provides a reliable basis for the research and development in this field.

Acknowledgments
This work was supported by General Planning Subject of the 13th Five-Year Plan for Educational Science in Jilin Province, project name: Research on the Construction of Diversified and High-level Cold Chain Logistics Specialty in Transforming Universities of Jilin Province, project approval number: GH180623.

References
[1] Wang Xuren, Bi Xueyu, Xu Weisheng, et al. Design and Implementation of Real-Time Network Security Monitoring System. Computer Engineering, Vol. 4 (2005) No. 118, p. 209-211.
[2] Tang Fangcheng, Yang Xiaohu, Dong Jinxian. Research on Network Security Monitoring System Based on Intelligent Agent. Computer Engineering, Vol. 12(2002) No. 28, p. 63-65.
[3] SHEN Jianyu, LI Jianhua, ZHANG Yueguo. Network Security Incident Monitoring System
Based on Event Flow. Information Security & Communication Security, Vol. 2 (2010) No. 1, p. 92-95.

[4] WANG Peng, CHENG Yanzhen. Application of Application Layer Protocol Recognition Technology in Network Security Monitoring. Digital Technology and Applications, Vol. 5 (2012) No. 12, p. 169-169.

[5] Hai Mo, Xu Zhengquan, HAI Mo, et al. Application of UML in Modeling of Network Security Monitoring System. Modern computer, Vol. 1 (2014) No. 17, p. 29-32.

[6] Huang Kejun. Research on Network Security Monitoring Model Based on Artificial Immune. Journal of Qinghai Normal University (Natural Science Edition), Vol. 2 (2010) No. 26, p. 70-72.