Application of Authentication and Secret-key Distribution Mechanism of Challenge-response in Micro-service Security Supervision and Authentication Interaction

Chang Chunlei, Bai Liang, Yun Kai, Li Kai*
State Grid Xinjiang Information and Telecommunication Company
Urumqi, Xinjiang 83500
*likai@xj.sgcc.com.cn

Abstract: The aims are to ensure the safety of communication among micro-service system modules, protect the trust of inter-servant-module, and improve the communicating efficiency. The authentication and secret-key distribution mechanism of challenge-response are introduced to improve the scheme for secure communication, supervision, and forewarning of data, and the effect is then tested. The modules of authentication and secret-key distribution and the data security communication are built according to the characteristic of challenge-response. These modules orient micro-service secure communication protocol. Besides, supervision and forewarning scheme is improved by running the log. Next, the security and efficiency of communication encryption and the function of supervision and management are tested. The results indicate that the scheme proposed can ensure the confidentiality and integrity of the communication process, and the log analysis module designed can promote and guarantee the daily operation and maintenance of administrators. Such progress has important reference value for applying authentication and secret-key distribution mechanism of challenge-response in micro-service security supervision and authentication interaction.

1. Introduction
In this information age, software development has mushroomed and thereby prompted industrial needs. Against this backdrop, Micro-service emerges as a new tool. Compared with traditional service systems that suffer limitations in architecture, micro-service is more compatible, more independent and therefore more popular in the Internet industry, among which is the software development sector [1]. The systematic shift, however, is bound to meeting problems, and relevant studies on this field are rare and theories are lacking, so the problems of the micro-service system become even more prominent. For instance, micro-service is a system consisting of many service modules. Though it features flexibility in operations, its structure that lacks inter-connection makes it difficult to maintain its operations; besides, information transfer among the modules in the micro-service system does not entail other media or complicated operations, which makes the communication vulnerable to attacks [2]. Because of these problems, the micro-service modules face tremendous security threats during data transfer.

To address these problems, this paper employed the challenge-response method and symmetric encryption to create a specific authentication control centre and make the communication of the micro-service confidential; meanwhile, a corresponding monitoring and early warning solution was proposed. This study intends to improve the security of data communication between micro-service modules and provide reference for further studies.
2. Method

2.1. Design of the authentication and key dissemination module
This section introduces the encryption of data transfer based on the dissemination of security keys. As the challenge-response method has the feature of zero knowledge and is easy to perform, it is used in this paper for identify authentication of the user and the session keys are disseminated scientifically [3]. The contents of the authentication and key dissemination module are as follows.

1) The client C and the authentication control center own the same key K; C is represented by the service name ID c in eureka (the registration and discovery center). When C makes a challenge-response request to S, ID c is attached and the timestamp T c is added, as shown in Eq. (1):

\[ C \rightarrow S: ID_c \parallel T_c \] (1)

2) S retrieves ID c from the registration center to confirm the legitimacy of the request, then generates the challenge code N to respond to C. In this process, K should be added as the key to confirm the information of the server that performs hash-based message authentication code (HMAC) to N and T c [4], as Eqs. (2) and (3) show:

\[ S \rightarrow C: T_S \parallel N \parallel Authenticator_S \] (2)

\[ Authenticator_S = HMAC_K(N, T_S) \] (3)

3) When C receives the response, HMAC abstract computation is performed on N and T c, and the information is compared with the verification information of the server to verify the identity of S. If the verification passes, C generates a new T c, uses K to perform HMAC abstract computation on the new T c and N, and then sends the new T c to S, as shown in Eqs. (4) and (5).

\[ C \rightarrow S: T_c \parallel Authenticator_C \] (4)

\[ Authenticator_C = HMAC_K(N, T_c) \] (5)

4) When S obtains the parameters, it performs the same abstract computation on N and T c to verify the identify of the micro-service client. If the verification passes, S performs Hash abstract computation on T c+1, the timestamp obtained by S, and K. The result is taken as the key to perform symmetric encryption of the session key SK and then sends the encrypted session key to the client, as shown in Eq. (6):

\[ S \rightarrow C: E_{H(N, K)}(T_c + 1, SK) \] (6)

5) The client performs the same Hash abstract computation to obtain the decryption key, thereby obtaining the session key SK.

2.2. Design of the data security communication module
Each successfully verified micro-service has a specific session key, which will be updated every two minutes, so that the information transfer between the microservice modules is safe and prevent the attackers from guessing and obtaining the key [5]. The data communication module is designed as follows.

1) The inquiry messages sent by the microservice A requires encryption, and ID A, T A and Authenticator A are attached, so that data transfer with the microservice B can be realized, as shown in Eqs. (7) and (8):

\[ A \rightarrow B: ID_A \parallel T_A \parallel Authenticator_A \parallel E_{SK_A}(M) \] (7)

\[ Authenticator_A = HMAC_{SK_A}(ID_A \parallel T_A) \] (8)

2) When B authenticate the identify of A, the Authenticator A should be attached to authenticate the identity to obtain the session key SK A to request A from the authentication control center (ACC), as shown in Eqs. (9) and (10):

\[ B \rightarrow ACC: ID_A \parallel ID_B \parallel T_B \parallel Authenticator_B \] (9)
3) ACC performs symmetric encryption on SKₐ with SKₐ, i.e., the session key of B, and then responds to B, as shown in Eq. (11):

\[
ACC \rightarrow B: E_{SK_B}(SK_A, T_S)
\]

4) B performs authentication using the computation parameter SKₐ, and enters the normal logic after the authentication passes.

5) When B responds, the same procedures are performed to realize response encryption.

When A tries to transfer data with B, it encrypts the data before making a request. The encryption process is shown in Figure 1.

![Encryption process diagram](image)

The response encryption module uses K₉. When A receives response, it performs authentication on the response source, and when the authentication passes, it sends requests to ACC to obtain K₉ to decrypt the data.

2.3. Monitoring and early warning solution based on operation logs

When designing the monitoring and early warning solution, this paper collects data by the method as shown in Figure 2.
Based on data collection, this paper designs an automatic monitoring mechanism consisting of two modules — the log analysis module and the early warning message module. In the design of the monitoring mechanism, the visits to the service and error rate are considered, and the early warning threshold is set. The design comprises three parts: analysis of the number of logs, analysis of the log changes, and analysis of the log error rate; when anomalies are detected in the system, the early warning program is started [6]. The early warning process is shown in Figure 3.

As per the process in Figure 3, this study sorts and analyses operation logs of microservices, so that the maloperations of the users can be detected, and the load condition of the service modules can be obtained.

3. Results and discussion

3.1. Security test of communication encryption
The testing tools Wireshark and Burp Suite are sued to test the security and integrity of the data during key dissemination. Wireshark is used to sniff the data and measure the possibility of obtaining effective
information from the communication data packet; Burp Suite intercepts and modifies the content of the data and measures the success rate of data replay [7].

1) Sniffing by Wireshark. In session key dissemination, the result of sniffing of data packets is shown in Figure 4.

As Figure 4 shows, the only effective information obtained from the data packet is the microservice ID, but the mere ID is not enough to fulfil the subsequent penetration task. Thus, key dissemination should be confidential.

3.2 Testing of communication encryption efficiency

This section will compare the effect of unencrypted communication, challenge-response encrypted communication, and hybrid encryption communication. The key dissemination response time and the communication response time of these three communication schemes are compared. The cache is deleted in the testing process.

1) Testing of key dissemination efficiency. Figure 5 compares the time of 20 tests by the proposed scheme and the hybrid encryption method.
As Figure 7 shows, the proposed scheme slightly outperforms the hybrid encryption method in the key dissemination process.

2) Comparative tests of communication efficiency. Figure 8 shows the communication response time of 20 tests of the unencrypted communication scheme, the proposed scheme and the hybrid encryption scheme.

As Figure 6 shows, the impact of the encryption schemes on the communication efficiency is within an acceptable range. Moreover, because both the proposed scheme and the hybrid encryption scheme adopt the symmetric encryption mechanism, the test result meets the expectation.

3.3. Testing of the monitoring and management function

This section tests the management function of the administrator. The administrator relies on the log analysis module to acquire the analysis data, compares the analyzed data, circumvents the detection log, and detects anomalies by the microservice ID and the log time. The monitoring center sends early warning mails to the administrator when the quantity of abnormal data exceeds the threshold, and the warning records will be stored in the control center. Collaboration between the early warning center and the administrator can effectively detect anomalies in a targeted manner.
4. Conclusions
This paper adopts challenge-response authentication and key dissemination mechanism to improve the security monitoring and authentication interaction of microservices, designs a relevant authentication and key dissemination module, a secure data communication module, as well as monitoring and early warning scheme. By using Wireshark and Burp Suite, we tested the modules, and confirmed that the proposed modules could effectively improve the security of encryption and data integrity. Moreover, compared with the unencrypted scheme and the hybrid encryption scheme, the proposed scheme has better performance in the efficiency of key dissemination and communication response. The study verifies that impact of the challenge-response authentication and key dissemination mechanism on the security of communication encryption and on the monitoring administration, thereby facilitating future studies in the microservice context. However, there are limitations. For instance, no comparative experiments have not been made with asymmetric encryption methods to compare the communication efficiency, and the pros and cons of encryption have not been explored. Future studies will be invested on these aspects.

Author
Chang Chunlei, male, November 1988, Han nationality, Qingdao, Shandong, Master's degree, senior engineer, research field: power information, cloud computing technology

References
[1] Esposito C, Castiglione A, Choo K K R.Challenges in delivering software in the cloud as microservices[J]. IEEE Cloud Computing, 2016, 3(5): 10-14.
[2] Kramer M, Frese S, Kuijper A. Implementing secure applications in smart city clouds using microservices[J]. Future Generation Computer Systems, 2019, 99: 308-320.
[3] Zheng Changan, Wu Xuezhi. A Study and Design of an Improved Short Wave Access Authentication System Based on Challenge / Response Mechanism [J]. Communications technology, 2015, 048(006): 729-733.
[4] Wang Haihong, Zhao Shengmei, Gong Longyan. Quantum Key Distribution Protocol [J]. Based on Challenge-response Mechanism Journal of Quantum Electronics ,2015(04):70-76.
[5] Qu Xia. A Study on Dynamic Password Identity Authentication System for SMS Based on Challenge / Response Mechanism [J].; and Software Guide ,2015,14(010):134-137.
[6] Pan Xiaoyang, Huang Xiaofang. Design [J.] of security control mechanisms for micro-service frameworks Journal of Southwest University of Science and Technology.
[7] Ding Xueying, Liu Di, Qiu Zhen. Design and Implementation of Application Monitoring System Based on Micro-Service Architecture [J]. Electricity Information and Communication Technology,2018,016(007):75-79.