A data security exchange method based on automatic arrangement

Zhenfei Qi1a*, Fuhua Zhang2, Feilu Hang1, Linjiang Xie1, Yue He1
1Information Center of Yunnan Power Grid Co. Ltd.
2Department of Science and Technology, Yunnan Power Grid Co. Ltd.
aqizhenfei@yn.csg.cn  *Corresponding author’s e-mail: chun_yany@163.com

Abstract. With the increasingly fierce attack and defense of network security, the security system needs to adopt the coordination of multiple functional modules to improve the security of the system. In practical application, web service protocol transmission and restful specification transmission can be used to ensure the security of data exchange. However, when the two protocols are used together (two security modules), it will cause great problems and workload to the security operation and maintenance. This paper proposes that the security function based on choreography which can distinguish the security operation sequence or script corresponding to the next step according to the protocol of the data package, and arranges the web service protocol and restful protocol together through script and engine to automatically coordinate work, so as to reduce the pressure of security operation and maintenance.

1. Introduction
With the continuous development of data communication network, network has become an indispensable part of people's life[1]. In the application of data communication network, many aspects of network security problems are gradually exposed, and the network security problems are increasingly prominent [2-3]. At the same time, with the increasingly fierce network security attack and defense confrontation, only relying on the prevention and prevention strategy can not guarantee the network security, we must pay more attention to detection and response[4-5]. This requires enterprises and organizations to build a new security protection system that integrates prevention, detection, response and prevention under the premise that the network has been attacked[6]. Therefore, there are many security systems which are coordinated by multiple functional modules.

"Design and implementation of distributed integration and data exchange platform"[7] designs a distributed integrated data exchange platform. The platform uses SOA and web technology to improve the traditional data exchange mode, more comprehensive centralized control of data exchange and ensure the security of data exchange. When the platform gets the data, it sends the request in SOAP message format through the service proxy interface. The SOAP message header adds the method of custom security attribute element. Use the HTTPS protocol to transmit data to avoid data theft and embezzlement. Through the coordination of soap module and SSL module, the security of data in the process of data exchange is effectively improved.

"Research and design of data exchange platform based on XML and web services" [8], system which improves the security of the system through soap, XML and private UDDI technology. When calling the soap request header of web service, the access speed and security are improved by using private UDDI. However, due to the requirement of data consistency in XML technology, data must
conform to specific schema. Although the scheme uses XML and web services to communicate through the firewall which can make the problems of data exchange and sharing in the system are effectively solved, there are still some problems about how to improve the efficiency of the system.

"Data sharing and exchange platform based on Web service" [9] puts forward a cross level and cross platform data sharing and exchange platform. The infrastructure of data sharing and exchange platform relying on cloud platform is based on SOA architecture, and Web Service technology is adopted for packaging components and application systems. The data sharing and exchange platform realizes data exchange and sharing through the service request and call of web service, and the resource user obtains the corresponding data through the REST API interface. The platform has good expansibility, but each module only adopts simple security technology, result in the security is not guaranteed.

"DiffSec: a differentiated intelligent network security service model" proposes the model of DiffSec security service which [10] adopts the NFV and SDN combined technology in order to design the structure of SANet and the corresponding intelligent control method. SANet, which is coordinated by two modules, can not only provide flexible and correct network security functions, but also have good network performance and practical value.

“The design and implementation of hospital data exchange platform based on rest Web Service” [11] mentions that project adopts both web service module and restful module, including database, management interface, audit interface, security operation and maintenance interface. Users need to configure and use the two modules; operation and maintenance personnel also need to be familiar with the two modules and maintain them. Security analysts need to analyze two sets of data. Because if there is a problem, it needs to be analyzed and traced in two modules.

In the existing schemes based on restful module and web service module, the internal security check is a different security series, which effectively improves the security of the network. However, the following problems exist in the above scheme:

- The multiple modules are independent of each other, and each module needs to be configured, inspected and maintained, it will result in high operation and maintenance costs;
- The system is not flexible enough in the process of operation. It needs manual operation in the process of problem analysis and so on, so the operation efficiency is lower than exception.

2. Proposed methods

Multiple security modules work together to deal with similar security problems. By unifying multiple modules into one module, the operation and maintenance pressure of the system can be reduced, and the workload of security analysts will also be reduced. To sum up, this paper proposes a security data transmission method based on choreography. On the one hand, multiple security modules are integrated into a system to reduce the pressure of system operation and maintenance. on the other hand, after the integration of multiple modules, the system can automatically find the corresponding security processing unit system according to the data package, without manual intervention, so as to improve the system efficiency. The security method based on choreography can also configure each module to dynamically modify the system to meet user requirements, as shown in Figure 1.

![Figure 1 flow of security choreography framework](image-url)
This paper provides a data security exchange method based on choreography, which is suitable for data exchange between different networks connected by gateways. The architecture of the method is shown in Fig. 2 and Fig. 3.

Figure 2 data security exchange method based on choreography

Through this method, multiple security modules can be integrated together through API interface and manual configuration to facilitate their automatic coordinated work, reduce the pressure of security operation and maintenance personnel, and facilitate users to use; the method architecture includes service API operation process, controller structure and process.

2.1. API operation process
The service API runs in the web security choreography filter web.xml Set in. The block diagram is as follows:

Figure 4 block diagram of safety layout filter
web.xml The configuration information is as follows:

Suppose the filter class is:

```java
public class SecuritySoarFilter implements Filter{}
```

```xml
<filter>
  <filter-name>SoarFilter</filter-name>
  <filter-class>SecuritySoarFilter</filter-class>
</filter>

<filter-mapping>
  <filter-name>SoarFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

The modules are as follows:

- Extraction of JSON parameters: protocol parameter protocol (text / XML corresponding to WebService) is extracted according to content type, token value is extracted according to token parameter, other parameters and request parameters are extracted to form JSON parameters;
- The controller is constructed by using the extracted JSON parameters, and the controller input parameters are JSON type;
- Running controller: run the run() function of the controller instance and return the JSON parameter, including {result, info};
- Return response: generate audit according to the operation results of the controller and return the response to the browser.

2.2. Controller structure and process

Task controller: it is responsible for extracting protocol configuration, forming script task table, running and returning results; see Figure 5:

- Extraction of protocol configuration: according to the input protocol number (extracted from JSON parameters), the configuration information corresponding to the protocol is extracted from the database. The data flow diagram is shown in Figure 5.

![Figure 5 configuration information extraction flow chart](image)

- The script task table: construct the script task table according to the configuration information table, traverse each entry of the configuration information, extract the parameter submodeparam of the security subtask from the JSON parameter according to the paramkey of each entry, call the corresponding security sub module construction function (using the parameter submodeparam and factory mode) according to the modetype of the configuration information table, and form the script task in the sequence of series Table. The data flow chart is shown in Figure 6:
• Safety sub module: normalize all modules used for safety inspection into safety sub modules and put them into module factory; module factory can construct security sub module instance according to module type (mode type of configuration information), and input parameters are paramkey from configuration information table and extracted from JSON parameters input; security sub module construction is completed and put into script task table for sequential execution. Each sub module contains run() function, which returns the JSON string {result, info};

• Task scheduling: after the script task table is constructed, it can be executed in sequence. When the control scheduler receives the result returned by the sub module as false, otherwise it will continue to execute the next sub module. The flow chart is as follows:

Figure 6 block diagram of script task list

Figure 7 task scheduling flow chart
• Protocol agent: Manage Protocol script, which is used to configure the security sub module information of a protocol. The configuration operation is completed by the protocol management module of intranet. The protocol management module submits the information to the protocol agent through the gateway, and the protocol agent stores the information into the database. Each protocol configuration can have many items. The controller will call the tasks represented by the corresponding parameters in sequence. Each task uses the sub module identifier to identify the type in the configuration item, and provides the parameter keywords passed in by the API interface, so that the security sub module can obtain the corresponding parameters.

![Figure 8 protocol configuration block diagram](image-url)

3. Conclusion
At present, security modules which based on Web service and restful protocol will appear in the scenario of secure data transmission between different security domains at the same time. However, the two modules work together to double the workload of security operation and maintenance, the complexity of security analysts' operation and the increase of workload, and the switching between systems will also lead to the increase of cost. In order to solve the above problems, this paper proposes a security data transmission method based on choreography, which can make the two modules work in one system. The security operation and maintenance personnel only need to maintain one system, and the security analyst only needs to deal with one system, which greatly reduces the operation and maintenance pressure of enterprise users.

References
[1] Zhou, Y.A. (2020) Technology changes life: right and wrong of "grass economy". J. Qunyan, 07:21-23.
[2] Wang, Y.Z. (2020) Research on data communication network maintenance and network security. J. Communication power supply technology, 37(02):206-207.
[3] Liu, X.M. (2020) Analysis of data information security technology in network communication. Communication power supply technology, 37(01):133-134.
[4] Mo, Y.J. Huang, J. Pan Y.J. (2020) Design and implementation of active defense system based on network security situation awareness. Journal of Medical Informatics, 41(03):60-63.
[5] Bai, X., Nurbuli., Wang, Y.D (2020) Research status and development trend of network security situation awareness. Computer Science, 47(S1):340-343+348.
[6] Jin, X.S. (2020) Design and implementation of medical network security monitoring platform. Computer Applications and Software, 37(02):322-325.
[7] Fang, C.P., Ma, K., Yang, B., Chen, Z.X. (2011) Design and implementation of distributed integration and data exchange platform. Journal of University of Jinan (Science and Technology), 25(01):11-14.
[8] Tang, J.W., Xun, H. (2006) Research and design of data exchange platform based on XML and Web Services. Microelectronics Computer, 01:14.
[9] Wei, J. (2018) Data sharing and exchange platform based on Web Service. Electronic Technology & Software Engineering, 15:149-150.
[10] Deng, L., We, W.N., Zhu, Z.Y., Chen, M. (2019) Diffsec: a differentiated intelligent network security service model. Journal of Computer Research and Development, 56(05):955-966.

[11] Gong, S.Y. (2017) Design and implementation of hospital data exchange platform based on rest Web Service. University Of Electronic Science And Technology Of China.