International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.77-88
http://dx.doi.org/10.14257/ijsia.2016.10.10.09

Implementation of Multi-level Network Security Management System based Middleware Strategy

Yunliang Zou

School of Business, Huaiyin Institute of Technology, Jiangsu, Huaian 223001, China
cloudzou@tom.com

Abstract

This article discusses the related art network security management, the proposed design of multi-level network security management system based on middleware ICE technology, the design of single-level system design and related species module of the overall framework for implementation. It is given based on the communication module ICE technology detailed design, it can be done from the LAN to the WAN, the communication between the various modules. The realization of various kinds at all levels of network security devices and associated host centralized monitor. Centralized configuration, through a variety of security-related information in a timely manner log collection management network species, real-time view of the network security status, dynamically adjusting network security policy comprehensive network security audit information, can effectively improve the overall security of network security management.

Keywords*: Security management; System policy; Network security; ICE distributed*

1. Introduction

Various safety devices such as firewalls, access control equipment applied to a large number of network information, type and quantity [1, 2]. But security incidents still showing growing trend seen, a simple pile of very effective security products micro indeed, as many security experts said, the security issue is not just a technical problem but a problem of management [3-5]. These safety devices isolated dispersed on the network, if no one can for the health of these devices, deployment, security event unified management system [6]. The security manager cannot be a comprehensive monitoring and management of the security situation in the entire network, and thus cannot guarantee the security of the entire system [7]. Only a firewall, intrusion detection, firewall, antivirus, authentication, and so audit the techniques combine collaboration in a unified security management platform in order to better protect your network [8, 9]. Research on network security equipment management will form a network security management system [10].

Multi-level security management system is based on a local area network or a single-level network management system based on the extended to the entire range of WAN [11, 12]. Thus all the many separate management system cascaded together to form a unified strict subordinate management relations through the event focused on multi-level distributed [13]. Policy and vulnerability management, can effectively improve event processing and statistical analysis across the entire network, centralized production and distribution of security policies in a timely manner to achieve full network security bug fixes, to improve the security of the whole network defense capability and security management efficiency have a significant effect [14]. Major worm emerged in recent years has distributed feature that can spread throughout the world in a very short period of time [15]. Network attacks are often from multiple

ISSN: 1738-9976 IJSIA

different networks, regional, or countries, making tracking and coordination of a wide range of defense needs [16, 17].

With the rapid escalation of network activity diversification and computer hardware, security management system is also required to have good scalability and high security. For the purposes of safety equipment and a host, including different systems of different platforms, be able to compare easily incorporated into the management system. ICE middleware technology gives a good solution, this paper design network security management system, using the ICE middleware technology as a communication module, complete distributed communications agency, to implement the system communication between the modules, while security incidents, the use of real-time publish-subscribe event, solves the problem of real-time security event. Advantages for ICE technology, proposes a multi-level network-based ICE security management, seems to apply to multiple management systems with distributed management systems for wide area networks, it is not limited to a specific network environment, enhancing the system scalability.

2. Related Method and Theory

Middleware is located at a software layer between the operating system and application software, he provides services to a variety of software applications, so that different application processes can block out platform differences in the situation, communicate with each other through the network [18]. Middleware is a use distributed software management framework API defined with powerful communications capabilities and excellent scalability, middleware play a connecting role in the three-tier structure, can greatly improve development efficiency and reduced application development time and effort, improve application the success of the development [19, 20].

2.1. ACE Framework

ICE is an object-oriented middleware platform. Basically, this means that ICE application for building object-oriented client server model provides the communication tools, application programming interfaces and libraries support .JCE client and server system framework shown in Figure 1, but with a definite link with the COBRA difference.

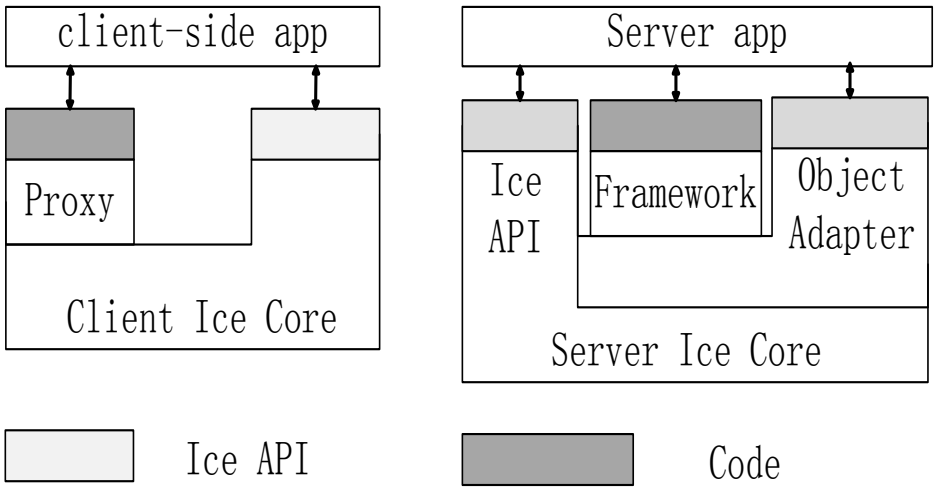

Figure 1. ICE Client and Server Architecture

Name of the client and the server does not correspond to a particular part of the strict allegations, but during a request from the occurrence to the end, some parts of the application assumed role. Clients are active entities that request to the server the server is a passive entity that provides services in response to client requests from the server not request, but only in response to the request of the angle of view, many servers are usually not pure server. It often acts as a server of some customers, but in order to complete their customer request, they will act as a client to another server similar to this, in the sense of merely requesting service, clients often are not pure client: they are often a mix of clients and servers, for example, customers can on the server starts a long-running operation, when starting the operation, customers can provide callback object to the server for the server to notify the client when the operation completes. In this case, the client acts as the starting operation customers, and upon receiving the operation is complete notification act as a server.

2.2. Firewall Module

Used by the operating system Linux, packet filtering firewall is implemented module, and its role in the system before or router forwards the packet intercept data packets. From Figure 2, packet filtering firewall module between the network layer and the data link layer. Because the data link layer is the de facto network card (NIC), the network layer is the first layer of the protocol stack, the packet filtering firewall software operating system is located at the bottom level.

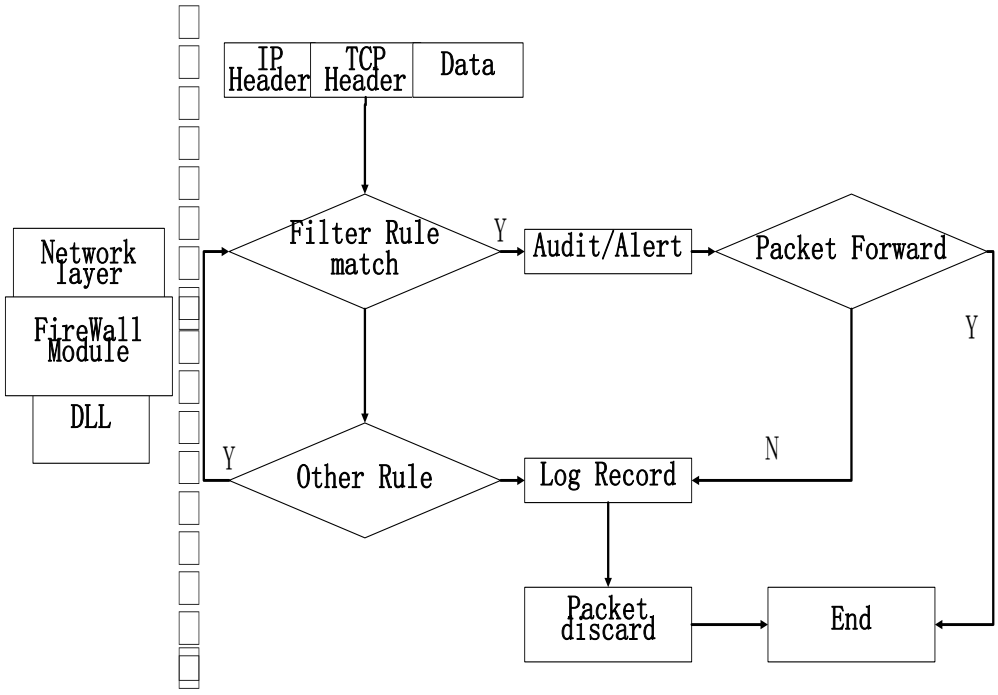

Figure 2. Firewall module

With this module, firewall can intercept and inspect all outgoing and incoming data. Check the firewall module first verifies whether the packet filtering rules, regardless of whether the filtering rules, the firewall generally recorded data packet, the packet does not conform to the rules of an alarm or notify the administrator. The module can check all the information in the package, usually a head at the network layer of the IP header and the transport layer generally include: IP source address, IP destination address,

protocol type, TCP or UDP source port, TCP or UDP purposes port, ICMP message type, TCP header some flag and so on.

2.3. Encryption and Authentication Technology

The basic idea is to disguise information encryption technology to make unauthorized access to fail to understand the true meaning of the information. Generally include password encryption algorithm design, code analysis, security protocols, authentication, message confirmation, digital signatures, key management, key escrow, so that the transmission of information security to protect large networks the only means of achieving. It is the core of information security technology; the general model shown in Figure 3:

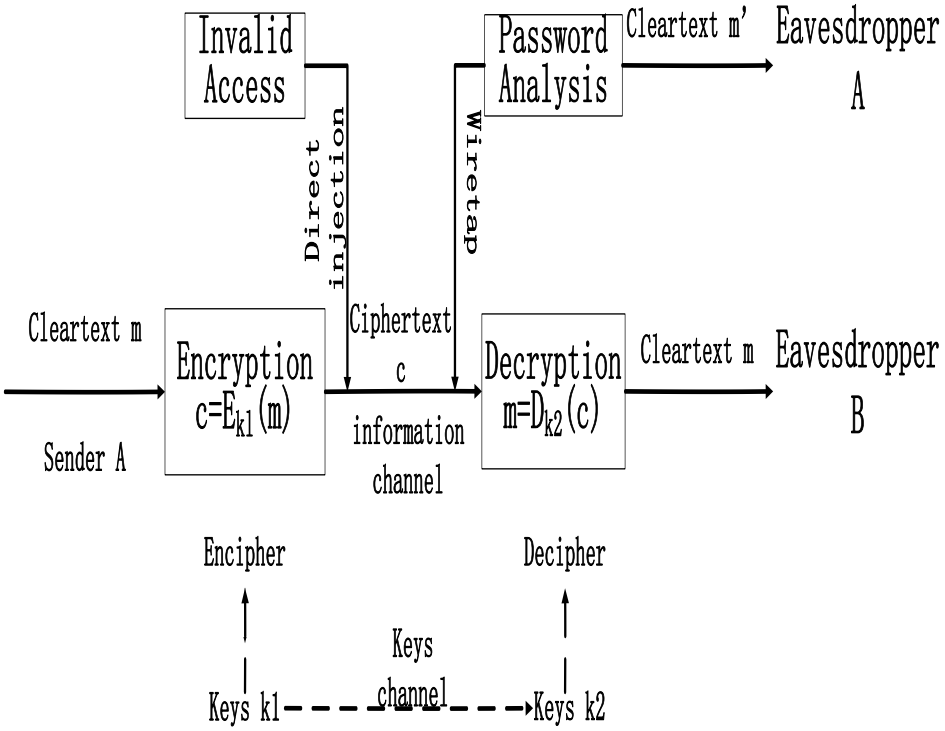

Figure 3. General Communication System Model

With respect to cryptographic techniques to conceal the contents of the message and the purpose of authentication technologies are: authentication message integrity authentication, authentication, and message number and the time of operation, which is mainly to prevent lawless elements of information systems active attack children.

A secure authentication system should at least meet the following conditions:

1) The receiver can verify and confirm the legitimacy, authenticity and integrity of the message.

2) The sender of a message issued by the message cannot deny sometimes required message recipient can not

Acknowledgment message received.

3) In addition to the legitimate sender of the message, the other person cannot send a message forgery.

3. Network Security Management System

3.1. Open Management Framework

In order to achieve a variety of network security devices to communicate with each other and linked in order to achieve overall security, firewall security vendors led to propose an open management framework. Internet security open platform through an open management framework, inherit and manage all network-related security content. In addition, it also provides a range of industry standard protocols based application programming interfaces (APIs), enabling users to easily integrate all based on the standard security applications such as access control, address translation, authorization, encryption, security auditing. Any third-party security systems in the series based on the programming interface developed can be inherited to the OPSEC framework structure. Once the addition OPSEC application framework, all network security can easily through the security policy editor to complete the relevant framework Figure 4:

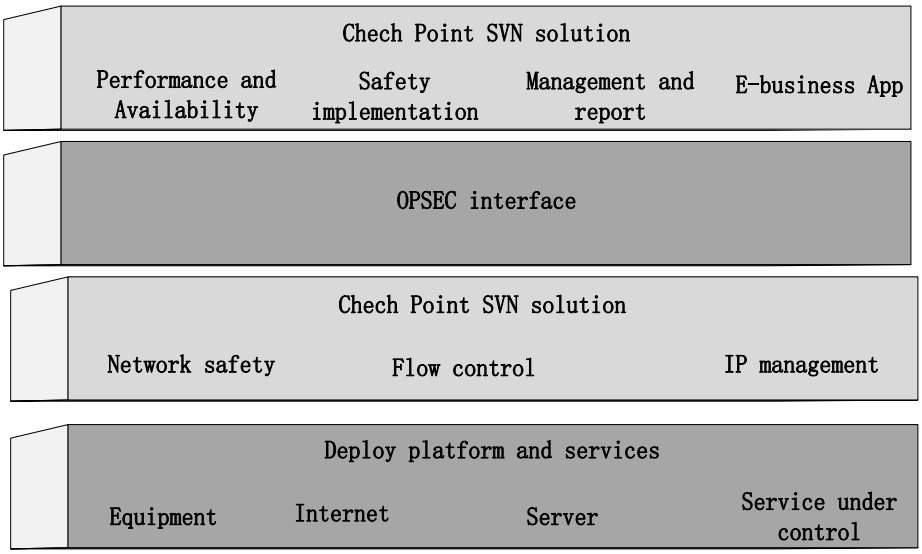

Figure 4. Integration of Multiple Security Technology

OPSEC application framework allows the entire enterprise network security tasks into completed by different security products, each product can be provided and installed on different devices by different manufacturers safety. Such as the advantage of better solve compatibility issues and the distribution of the load process, but also has high flexibility, enabling managers to choose the best security products based on enterprise network security needs, as well as conducting a security operation of the product update when not affect the normal operation of other products.

General network security management of three-layer structure was shown in Figure 5. Communicate with each other, the paper is used by specific communication protocol is ICE communication. In the name of a management terminal administrator of managed objects and management domain server management, user management terminal directly to administrators need to provide easy to use, graphical interface. The management information formatted output, and according to a certain logic to enter the administrator interface for processing, online management terminal can accept information management domain managed object server forwards the report, events in real-time prompts the administrator user is currently happening.

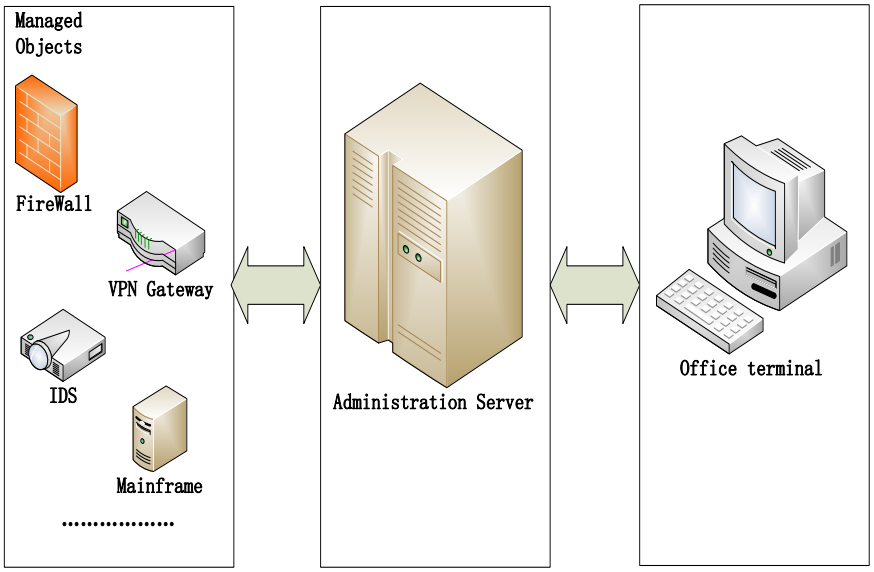

Figure 5. Network Security Management Layer Chart

Management domain server is the center of the three-level management model, which is a collection of the whole network security management information system architecture to express its unified management of information resources available to manage the terminal, and the management information from each terminal visit, directed to the corresponding managed object based on certain policies. "So from the perspective of the management terminal management region server centralizes all information management domain servers it can manage is a huge management objects, which also includes its own management itself information object Manager domain secure domain server as an event response center, responsible for receiving incident management objects, and in accordance with pre-established policy to respond to events, the response should include: recording, alarm or respond to, manage domain server notify the appropriate administrator or line management terminal according to policy and permissions management or other objects to be adjusted.

3.2. Device Management

The module of the completion of the security device system relationship unified configuration and display all safety equipment, workstations running, the network communication status of each device to ask, fault alarm, coordination linkage. Each level supervision center only safety equipment directly connected to management (Figure 6).

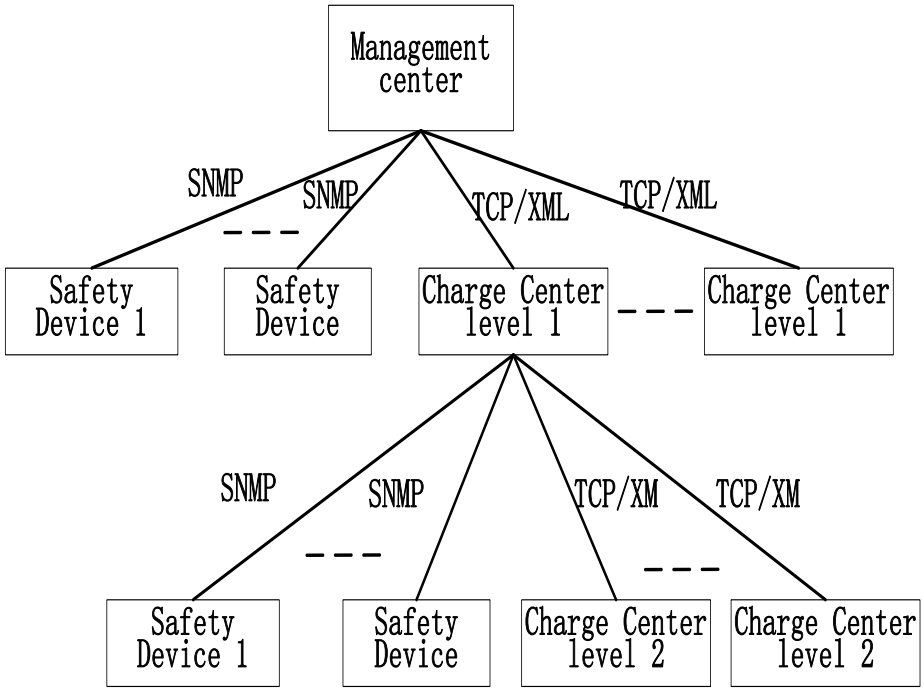

Figure 6. Equipment Distribution Topology

Each monitoring center directly connected devices using the SNMP protocol to obtain device status information, charge information center for superior monitoring center reporting, and through XML technology for data conversion and transmission. Superior topology map to display topology information center in charge of the relationship with each level topology based on real-time information you want to increase or decrease the device, modify the status of the communication between devices, and display refresh.

For each level security management system abstraction, it is mainly composed of the console. This general security management system is substantially the same, except that the system uses ICE Middleware communications module, has great scalability. Each part of the function is also consistent with the general NMS, increased monitoring of LAN hosts.

4. Experiments and Results

4.1. System Framework Design

In this structure, each security control center in addition to the management of this site safety equipment, but also the lower sub-management safety control center. In this way, it can all subnets and the security control center regarded as a peer lower network structure, making the development and management of operation and maintenance costs, and the system structure is clear. Because each subnet is full reciprocity, that is where network security devices, hosts, *etc*. are part of the same internal LAN for any or a single-level network security management system, which is the same as the frame knot enough.

Physical frame system is shown below Figure 7. To form a strict management of superior-subordinate relationship for a security management and a statement, in addition to the present level of security and a host device, its right to administer two, tertiary safety management system that can send commands to them, collect twenty-three security log Secondary security management, in addition to the level of the host and the security device, you can only manage their subordinates three security

management system, sending commands to the lower or collect subordinate security log. Three security management system is only responsible for the management and host security apparatus of the present level within the same time reported the same level of security incidents.

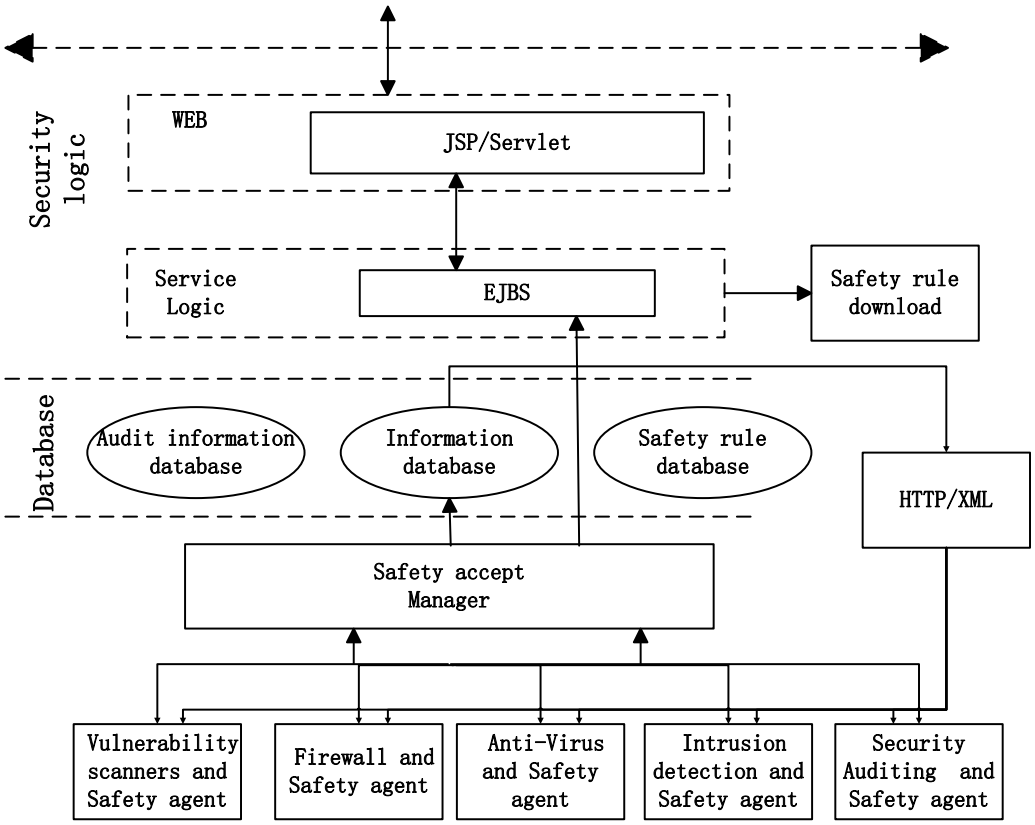

Figure 7. Cross-Level Security Management System Framework

4.2. Communication Centers and the Role

Communication center of the whole system is a communication module managers, including some of the major two functions: one for cross-level commands transmitted management and forwarding; second is to provide event server to collect and forward security events to set the communication center. the purpose of the communication module for connection management to effectively utilize the bandwidth, which is mainly reflected in the use of cross-level communication. For users of the upper, the communication center is transparent. Communications centers do not provide an interface to the upper layer user. Configuration and implementation on the ground floor so are completed. Communication Center maintains a list that shows the correspondence between the id and connection, taking into account the characteristics of ICE, the communication center of the list format as shown in Table 1:

Table 1. Message Center Link

Id	Identifier string	Proxy
123	192.168.1.92:6789@local	The proxy to the 6789 port of 1.92
234	192.168.1.92:9999@local	The proxy to the 9999 port of 1.92
12345	192.168.1.92:9999@192.168.2.92	The proxy to the 9999 port of 2.1

The method has been adopted in order on the list can send cross-level communication by id command message directly to the target host, making the transfer process more convenient, avoiding the need to create each connection destination was connected unnecessary overhead, and for communication between the local level, its effect is not very obvious.

4.3. Cross-level Communication Decomposition

Due to the nature of the cross-level communication, data string is transmitted via the communication center are forwarded to the destination host. Therefore, cross-level communication flow chart shown in Figure 8:

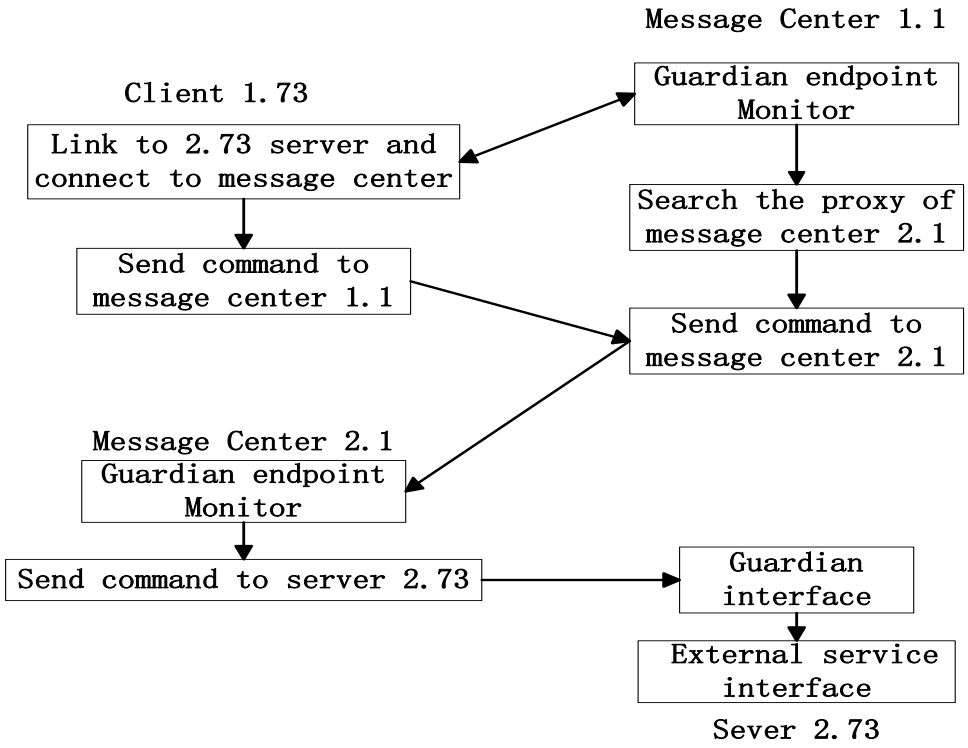

Figure 8. Cross-level Communication Frames

1) 1.73 to establish a connection with the communication center of the stage 1.1, and will identify the destination address is sent to the communication center, namely: 192.168.2.73: 9999@192.168.2.1.

2) Identification 1.1 communications center will resolve the received, determine whether cross-level communication center, create or find ICE agents 2.1 Communication Center locally maintained list, and the id back to the client 1.73.

3) 1.1 Communication Center will become the connection identification 192.168.2.73:9999@192.168.2.1 reassembled 192.168.2.73:9999@loeal, and the ID to 2.1 communication center.

4) 2.1 communication center sent over the connection identifier is parsed to determine the purpose of the next stage after the host-based host, create or generate 2.73 to 2.1 workers in the local CE Agent communications center maintained list.

5) 1.1 communications center to get a connection id 2.1 communications center returned.

Conclusions

The proposed design of multi-level network security management system based on middleware ICE technology, the design of single-level system design and related species module of the overall framework for implementation. The realization of various kinds at all levels of network security devices and associated host centralized monitor! Centralized configuration, through a variety of security-related information in a timely manner log collection management network species, real-time view of the network security status, dynamically adjusting network security policy comprehensive network security audit information, can effectively improve the overall security of network security management. With the further development of the network and security technologies, the demand for network security management is also growing, in order to reduce development costs and management costs of network security management and unified interface to solve the problem of different platforms, different systems and different devices, become the main trend. Similarly ICE advantage of this aspect will be further developed.

References

[1] Su B., Yang J. and Wang B., "Information Sharing System of Ad Hoc Networks: Based on Data Access Service[J]", **(2015)**.
[2] M. Henzinger, "Link Analysis in Web Information Retrieval", IEEE Data Engineering Bulletin, **(2000)** Sep., pp. 3-8.
[3] Kučera A. and Pitner T., "Semantic BMS: Ontology for Analysis of Building Automation Systems Data[M]",//Technological Innovation for Cyber-Physical Systems. Springer International Publishing, **(2016)**, pp. 46-53.
[4] M. Sadek, A. Tarighat and A. H. Sayed, "A Leakage-based Precoding Scheme for Downlink multi-user MIMO Channels" , IEEE Transactions on Wireless Communications, vol. 26, no. 8, **(2008)**, pp. 1505-1515.
[5] Wu L., Xue L. and Li C., "A Geospatial Information Grid Framework for Geological Survey[J]", PloS one, vol. 10, no. 12, **(2015)**.
[6] Z. Yazhou, Z. Guoxin, R. Yun and L. Mingqi, "A Novel Distributed Precoding Scheme Based on THP for Downlink Multi-Cell Multi-User OFDMA Wireless Systems", IJACT: International Journal of Advancements in Computing Technology, vol. 5, no. 9, **(2011)**, pp. 213-220.
[7] Fengguang X. and Xie H., "Networked Automatic Test System based on Message-oriented Middleware [J]", International Journal of Control and Automation, vol. 8, no. 3, **(2015)**, pp. 147-160.
[8] R. Soungalo, L. Renfa and Z. Fanzi, "Evaluating and Improving Wireless Local Area Networks Performance", IJACT: International Journal of Advancements in Computing Technology, vol. 3, no. 2, **(2011)**, pp. 156-164.
[9] Li Y., Zhang Y. and Li P., "An Efficient Trusted Chain Model for Real-time Embedded Systems[C]", //2015 11th International Conference on Computational Intelligence and Security (CIS). IEEE, **(2015)**, pp. 428-432.
[10] T. Okamoto, "A digital multisignature scheme using bijective public-key cryptosystems", ACM Trans. Computer Systems, ACM Press, New York, vol. 6, no. 4, **(1988)**, pp. 432–441.
[11] Hart S. M., Interface for use with a video compression system and method using differencing and clustering: U.S. Patent 8,990,877[P]. **(2015)** March 24.
[12] A. Boldyreva, "Threshold signature, multisignature and blind signature schemes based on the gap-Diffie-Hellmangroup signature scheme", In Proceedings of PKC 2003, LNCS 2567, Springer, Berlin, **(2003)**, pp. 31–46.
[13] Hart S. M., Interface for use with a video compression system and method using differencing and clustering: U.S. Patent 8,990,877[P], **(2015)** March 24.

[14] M. Bellare and G. Neven, "Identity-Based Multisignatures from RSA", In CT-RSA, 2007, LNCS 4377, Springer, Berlin, **(2007)**, pp. 145–162.
[15] C. Gentry and Z. Ramzan, "Identity-BasedAggregate Signatures", In PKC 2006, LNCS 3958, Springer, Berlin, **(2006)**, pp. 257–273.
[16] Ferdaus M. H., Murshed M. and Calheiros R. N., "Network-Aware Virtual Machine Placement and Migration in Cloud Data Centers[J]", Emerging Research in Cloud Distributed Computing Systems, vol. 42, **(2015)**.
[17] D. Boneh, C. Gentry, B. Lynn and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps", In Proceedings of Euro-crypt 2003, LNCS 2656, Springer, Berlin, **(2003)**, pp. 416–432.
[18] A. Boldyreva, C. Gentry, A. O'Neill and D. H. Yum, "Ordered Multisignatures and Identity-BasedSequential Aggregate Signatures with Applications to Secure Routing", In Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM Press, New York, **(2007)**, pp. 276-285.
[19] Zou H., Qian Y. and Zhao Y., "The Design and Implementation of Data Security Management and Control Platform[M]",//Applications and Techniques in Information Security, Springer Berlin Heidelberg, **(2015)**, pp. 368-378.
[20] C. Y. Lin, T. C. Wu and F. Zhang, "A Structured Multisignature Scheme from the Gap Difffie-Hellman Group", Cryptology ePrint Archive, Report 2003/090, **(2003)**.

Author

Yunliang Zou, he received his M.A. in Art from Sichuan Agricultural University. Currently, he is a manager of computer lab, school of business, Huaiyin Institute of Technology. His current research interests include Management and Network Security.