Research on Aggregate-Type Network Communication System Based on Information Sharing

LI Yue[1, a], PENG Zuhua[1, a],XU Chao[1, a]

1 State Grid Xinyang Power Supply Company, Henan, Xinyang

[a]55609170@qq.com

Keywords: network information; aggregate-type; network communication system**.**

Abstract. Under the Web 2.0 environment, to break isolation between sites and share information is the development trend of network media as well as the objective needs of netizens. Some network operators have researched on this, however, the four traditional communication programs, server agent, dynamic creation of script, segment identifier communication and Flash technology, have low efficiency, transmission quality and security. Therefore, based on cross-text communication technology, this paper builds an aggregate-type network communication system which depends on information sharing to improve the efficiency, quality and security of information aggregation between sites and provide netizens with more convenient service of information aggregation.

Aggregate-type Cross-domain Communication Program Design

The aggregate-type cross-domain communication program system in this paper first treats different websites or sites as individual trust domain, next encapsulates them to internal components which have interactive access and transmission ability, and then uses the new cross-text communication technology of HTML5 to achieve the communication activities between components. In this way, it can meet the requirements of convenient, effective and safe cross-domain information visiting. Specifically speaking, the latest version HTML5, developing from HTML, is added to another new cross-text communication mechanism or cross-text communication technology to meet the requirements of cross-domain information visiting between sites. It calls PostMessage in the iframes or specific window of message requirement transmitter, while sets up a event hander in receiving end to receive the message requirement signals to achieve information dock. The steps are as follows: first, call PostMessage in the iframes or specific window of information to send metadata requirement message of data, origin and source; next, assign the receiver or sender; last, add a event listener for message event in the receiving window of metadata requirement message to extract and return data. This method can guarantee accurate aggregated data and meet requirement of pre-fetch message aggregation. This method can guarantee accurate aggregated data and meet requirement of pre-fetch message aggregation.

The Safe cross-domain Communication System Based on Information Sharing

As shown in Figure 2-1, this safe cross-domain communication system consists of domain encapsulation module, inter-domain communication module and fine-grained object sharing module. These modules are the basic structures of this system.

Domain encapsulation module

Trust domain, also named trust site, refers to credible IP address or DNS website in aggregate-type network communication mode, security system is added to DNS domain. The components, mainly supplied by the third-party, are indentified as encapsulation of metadata in the same trust domain or trust site. They are logically independent, and have individual input and output port which offer essential interfaces to communication component between domains. Different components are for encapsulation of metadata in different trust domains to keep isolation between domains.

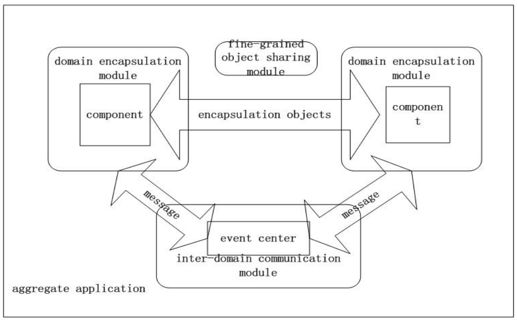
fine-grained object sharing module
domain encapsulation module
component
encapsulation objects
domain encapsulation module
componen t
message
message
event center
inter-domain communication module
aggregate application

Figure 2-1 Basic structures of safe cross-domain communication system

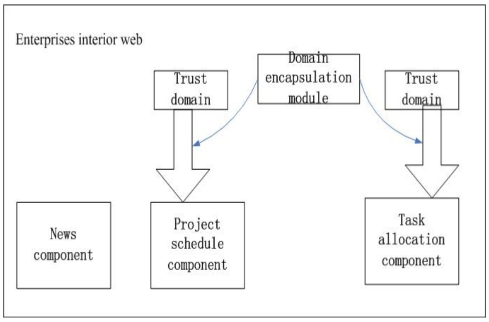
Enterprises interior web
Trust domain
Domain encapsulation module
Trust domain
News component
Project schedule component
Task allocation component

Figure 2-2 Structure of domain encapsulation

Figure 2-2 is the structure of domain encapsulation map for intranet of a news institution. On this website, news, forum blog, project schedule information and task allocation information are blended. Netizens can make free combination of these services by themselves and use them flexibly. First, project schedule information and task allocation information are respectively encapsulated in project schedule component and task allocation component to keep isolation between metadata in the two domains. Next, inter-domain communication system is used to achieve information access and feedback between domains. In this way, these two services, inter-domain isolation and communication, achieve the communication activities between different intranet sites of aggregate-type network communication system.

This system uses isolated components to improve security level in the whole system, that is to say, put different components in different iframes to ensure the independence of all components, then any component couldn’t modify domain and attack other components. For different trust-leveled metadata message in the same server, this system can create several DNS domains to isolate components and thus to guarantee security. For example, different trust-leveled metadata t1 and t2 come from the same server www.map-site.com, and then system can create two DNS domains, t1.map-site.com and t2.map-site.com, to encapsulate these two components, to guarantee effective inter-domain communication and system security. Compared with traditional communication system in network environment, cross-domain communication system in this paper has prominent advantages and can address common problems of low efficiency, transmission quality and security in traditional cross-domain communication system.

Inter-domain communication module

How to guarantee an effective communication process is a problem for this system design. For this goal, URL segment identifier can be adopted in the system. Therefore, system in this paper adopts cross-text communication mechanism to guarantee effective communication activities between components as well as component and aggregated applications.

From Figure2-3 running structure of cross-domain secure communication system, we can see that event center, on one hand, is responsible for creating and deleting channels, loading and unloading components as well as connecting interface channels with component ports; on the other hand, is used to process metadata message to and from all ports. In the cross-text communication layer, component cross-domain communication service and information aggregation application service are achieved here to guarantee effective interactions between component frames and channel frames. Event communication layer is used to transmit message from all components. In addition, Figure 2-3 shows the communication process between components and information aggregation application. The event center layer of information aggregation application service is used to send message to the output ports of components by special channels, and in event communication layer, message is sent to input ports of target component; while in cross-text communication mechanism, message is sent to component frames, when roll polling monitor find the message, the event communication layer of this component will use SECommClient (messageRecieved) to process the message, then it will use callback function to present the message. In this procedure, the effective communication process between component and information aggregation application services is achieved.

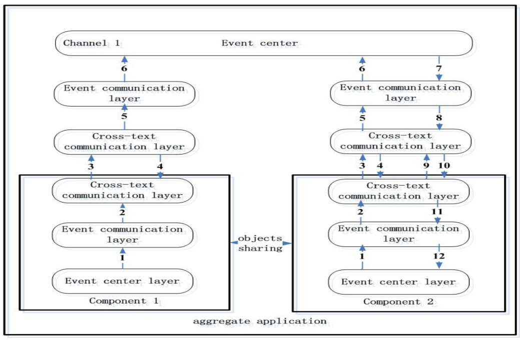
Channel 1
Event center
6
6
7
Event communication layer
Event communication layer
5
5
8
Cross-text communication layer
Cross-text communication layer
3
4
3
4
9
10
Cross-text communication layer
Cross-text communication layer
2
2
11
Event communication layer
objects sharing
Event communication layer
1
1
12
Event center layer
Event center layer
Component 1
Component 2
aggregate application

Figure2-3 Running structure of cross-domain secure communication system

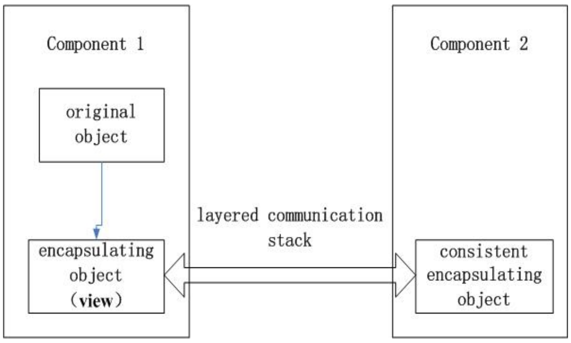
Component 1
Component 2
original object
layered communication stack
encapsulating object (view)
consistent encapsulating object

Figure2-4Encapsulating object view sharing process

Fine-grained object sharing module

From Figure 2-4, we can see that the secure cross-domain communication system uses object encapsulation strategy of JS Library to create an encapsulating object view, after serialization, the object is sent to component 2 by layered communication stack; while after receiving message, component 2 will deserialize it to be an object which has similar attribute with original object; then, it takes the channels of component cross-domain communication into practice. Fine-grained object sharing module has multiple functional values in transmission: on one hand, JS Library serializes and deserializes the object to achieve attribute conversion and transmission of objects between components; on the other hand, homologous strategies of different browsers guarantee the isolated processing between frames, while it inputs the asynchronization by layered communication stack when sharing remote objects. These technologies address many problems in object sharing transmission and improve the security of system. Therefore, fine-grained object sharing module is essential for secure cross-domain communication system.

Security Design of Aggregate-type Network Communication System

Generally speaking, Web page includes JavaScript and static document. JavaScript is either from the-third party page or from original text, so scripts have the same authority; while static document is expressed in Document Object Model (DOM). Based on existing literatures, this paper will use the encapsulating object view mechanism to further encapsulate fine-grained object sharing to avoid more access permissions and potential risk of malicious attack. When JavaScript is in original text, it shares global variable and a DOM, so it can access to this texts or other texts in the same domain, but not the texts in other domain. Reliable mechanisms like server script rewrite tool and frame tool of browser can encapsulate scripts to keep them isolated. First, under homologous strategy, if information aggregated procedure wants to embed applications which are from the third party in the home page, while browser couldn’t provide effective isolation and protection, therefore, system designer should use server script rewrite tool to make automatic certification and modification of the third-party procedures before embedding applications from the third party to achieve the isolation between home page of information aggregation and applications from the third party. Second, reliable platforms in system can make repeat encapsulation on components to effectively control the attack of JavaScript, while wrapper security mechanism can effectively solve non-holonomic strategy attack, non-complete arbitrate attack, non-reliable callback function attack and parameter type forge attack, so, to a large extent, it solves a series security risks in cross-domain communication system.

Aggregate-type Network Communication System Testing

This paper uses many parameter set to measure component numbers and effectiveness of roll polling interval on data throughput. The number of component increases from 1 to 32, while polling interval is supposed as 10m, 20ms, 40ms, 80ms. From the final result, we can see that information aggregated application system needs very short time to transmit small data volumes like 4KB, 8KB to components, but it needs much more time when data volume is bigger than 1MB. It also shows that with increase of component number, the throughput of aggregate-type network communication system which is based on website information sharing is increasing; what’s more, when component number is higher, the growth rate is lower. To evaluate the event rate, this paper adopts 15 characters, the standard load of small event, to be the load capability of test event in the system. And the specific testing is planned in this way. From the testing result, we can see that different browsers have different event rate but the similar development law. In other words, with the increase of component number and roll polling interval, event rates in browsers are increasing. In this system, with the increase of loaded component number, the delay time is shorter, particularly when browser caching is embed in Safari browser, the delay time is much shorter, so the whole system shows high efficiency and quality of component load. It makes information aggregation time between special websites become much shorter for netizens. In addition, testing the aggregate-type network communication system which is based on website information sharing and FIM system in browsers such as IE8.0, Safari4.0.5, Firefox3.6.3, Google Chrome6.0.401.1 and Opera10.54, we see that the load time of components in this system is much shorter than that in FIM system while this system is also much prominent in system operating efficiency.

Conclusion

The aggregate-type network communication system which is based on website information sharing in this paper has more improvements in data throughput and event rate while the delay time of component load is much shorter with the increase of component number, and the overhead of JS executive event in object sharing is limited, especially when the reliable platform and recursive encapsulation which are used in the system create encapsulation with double input and output, the security of system is much improved. All these advantages make secure cross-domain communication system in this paper have actual application value.

References

[1] Gao Bo, *Resource Sharing in Network Age*,M, Beijing Library Press, 2013(1).

[2] Li Weize, *Practice Strategy for Entrepreneur Information Platform*,M,Qinghua University Press, 2008 (11).

[3] Liu Xiaowu, *Network Security Situation Perceptual Model on Multi-Source Fusion*, J, Journal of PLA University of Science and Technology, 2012 (4)