A Time-Constrained Secure Data-driven Coordination Model

Hua-Ji SHI[†], Xue-Jun SHAO[†], and Xing-Yi LI[†,††]

[†] School of Computer Science and Telecommunication Engineering ,Jiangsu University ,Zhenjiang,212013 China
[††]School of Electronics and Information Engineering,Beijing Jiaotong University,Beijing,100044 China

Summary
The article mainly research the use of the security problem under the opening environment which the Linda-like data driven coordination model brings. In an open environment , it cannot guarantee all visit data coordination space the software entity credible. In order to carry on the control of the data coordination space security, it proposes one kind of security coordinated model with the time restraint. This coordinated model can realize coordinated tuple space safe access control by increasing the specific information to the tuple data and using mix key mechanism realization.

Key words:
Access control, Coordination, Hybrid encryption

1. Introduction

The coordinated model has provided one kind of description software entity interactive frame, at present in the open system coordinated technology, it mainly considered how urges software entity to be interactive successfully. But in fact, under the open system we cannot guarantee each software entity credible, based on the consideration of system safety aspect, it must have to have certain safe access control mechanism to limit interactive between the software entity.

At present, only KLAIM(De Nicola,1998) and the SecSOS(Vitek,2003) coordination language has provided certain safe access control mechanism. The KLAIM coordination language describes the software entity visit jurisdiction by the type, the access control strategy between the software entity and the tuple data, causes the software entity and the data to form one kind of 1 to1 corresponding the relations. And this method cannot satisfy the open system dynamic request well, nor support on the tuple data fine grain safety control. SecSOS control data visit only by increasing certain additional information to the spatial tuple data. This kind method of locks tothe field cannot only carry on the control to the entire tuple data, but also support data fine grain safety control. But the SecSOS flaw energy region can't differentiate two kind of different types of reading operation, and the data read can write in the similar data to the tuple data space. Nadia Busi,Roberto Gorrieri et al. have carried on the expansion on foundation of KLAIM and the SecSOS,and proposed the safe coordinated model SecSpaces(Busi,2003). But SecSpaces utilizes the asymmetrical key to carry on the match each time, and its' computation order of complexity is high, moreover it has not provided the effectiveness control, thus it reduced the system security. This article first introduces the data-driven coordinated model Linda(Gelernter,1985) model under the open system, then the simple introduces SecSpaces safe coordination model, afterwards it proposes one kind of new data-driven coordinated model with the time restraint security.

2. Linda Data-driven Coordinated Model

Under the open system, the correspondence between the software entity by using the coordinated technology is one extremely effective method. It can satisfy the open system Interoperability, the probability, the elastic request .In 1985, David Gelernte(Gelernter,1985) proposed architecture based on the data-driven coordinated model, Sun Microsystem and IBM Corporation has developed respective commercial product JavaSpaces and TSpaces on this foundation. These all use one kind called the regeneration correspondence (generative communication) pattern: The data transmitting end and the receiving end carry on the correspondence through a sharing data tuple space, the transmitting end send in the data this sharing space, the receiving end read data from the sharing space. The data sharing space is independent of any party, once the transmitting end send the data in the sharing space, the data does not belong to the data provider . Any receiving end may withdraw the corresponding data. The Linda model has defined three kind of elementary operation: out(e), int(t) and rd(t). Input operation out(e) is to write data item e inthe sharing tuple space; int(t) is to match template t and data item e in the sharing space if they discovery matched data item e, then will read e and delete e in the sharing space. rd(t) and int(t) are similar, but they merely read not delete. The Linda model definition match rule like defines 2.1.

Defines 2.1: Supposes $e =< d_1; \cdots ; d_n >$ is a data item, for matches the template $t =< dt_1; \cdots ; dt_m >$, if t and the e match must satisfy the following condition:

Manuscript received March 22, 2007
Manuscript revised March 28, 2007

(1). $m \le n$,

(2). $dt_i = d_i$ *or* $dt_i = null$, $1 \le i \le m$,

From defines 2.1,we can see the initial Linda coordination model not provide the corresponding safe access control mechanism to carry on the control to the read-write operation, also cannot differentiate int(t) and rd(t) with destructive operation.

3. SecSpaces Security Data-driven Coordinated Model

At present, only KLAIM and the SecSOS coordination language has provided certain safe access control mechanism. In 2002 Nadia Busi, Nadia Busi, Roberto Gorrieri have carried on the expansion and the revision to the two coordinated language of KLAIM and the SecSOS safe access control mechanisms. They proposed the SecSpaces model (support under opening environment safe data-driven coordinated model). SecSpaces not only can differentiate the read-write operation, but also can differentiate int(t) with non-destructive reads and rd(t) with destructively operation. SecSpaces attaches the specific control information to the tuple space data. Logical district field Partition, another asymmetrical logical district field Asymmetric Partition. The former differentiate tuple space in logical the district,it might increase not only the data security through this field but also the fast index to the corresponding data. The latter use the cryptology asymmetrical key to data reading to carry on the authentication of read-write operation, it can differentiate reads and writes strictly. Simultaneously the latter is divided into int(t) and the rd(t) region, it can distinguish these two kind of read-write operation.

4. Security Data-driven Coordinated Model with the Time Restraint

The safe access control mechanism which from the above SecSpaces model provides we may see:

(i) Each time read-write operation of data to can carry on the asymmetrical decipher operation, and the computation is complex.

(ii) Once some software entity obtained read some data key, it will obtain the permanent read power, SecSpaces has not provided the effectiveness control. To the dynamic open system is unsafe, for example a Agent entity leaves after reading data, it visit the corresponding data once more certain time, but this time Agent possibly already became unsafe, but it can still read depended upon the formerly key.

In view of SecSpaces existence security problem, this article proposed one kind of security data-driven coordinated model with the time restraint. We increase the time limit control field to the match template to control the time of the software entity visit sharing data space , and make the coordinated model time boundedness. Meanwhile using the mix key authentication mechanism replaces the asymmetrical authentication to reduce the complexity of SecSpaces computation.

The model safety control rule description is as follows: Project e and the template t definition is: Supposes project $e =< \vec{d} >_{[k]}^{[c]}$ c ∈ Partition,k ∈ APartition(asymmetric partition), $\vec{d}$ expresses the tuple data. Supposes template t= $< \vec{dt} >_{[kt]}^{[ct]}$ ct ∈ Partition, kt ∈ APartition. $\vec{dt}$ expressed the template data (usually expresses wildcard character with added value null). On the read match template the increase timing control field, supposes $T = \{bt, et\}$ as the time section, bt is the read starts the time, et is the read closure time, supposes t is the current time.

Defines 4.1:

Supposes e= $< d_1; d_2; ...; d_n >_{[r;s]_{rd}[r';s']_{in}}^{[c]_{rd}[c']_{in}}$ to take a project, t= $< dt_1; dt_2; ...; dt_m >_{[rt;st]}^{[ct][T]}$ took a template and supposes op ∈ {rd,in}. Other definitions with defines 2.1. Supposes ce and ct is and project e the correlation operation op control field, if satisfies the following condition, then project e and t in operates on op is matches:

(1) $m \le n$;

(2) $dt_i = d_i$ or $dt_i = null, 1 \le i \le n$;

(3) $c_e = c_t$;

(4) $bt \le t \le et$;

(5) if r = (k; p) then decrypt(st; k) = p;

(6) if rt = (kt; pt) then decrypt(s; kt) = pt;

Below looked how carries on the access control through the asymmetrical key, as shown in Table 1.

In supposition (1),(2),(3),(4) condition satisfied situations, (PrivKA; PubKA) and (PrivKB;PubKB) is two pair of keys respectively is the private key and the public key.

Table 1: Asymmetrical key access control

Template (t)	Data item	Whether matches
<null>[?;{p}PrivKA]	<d>[(PubKA;p);{pe}PrivKB]?	Y
<null>[(PubKB;pe);{p}PrivKA]	<d>[(PubKA;p);{pe}PrivKB]?	Y
<null>[?;{p}PrivKE]	<d>[(PubKA;p);{pe}PrivKB]?	N(if PrivKE ≠ PrivKA)

In order to guarantee the time pokes itself security, it may carry on the encryption by using key k to T, current time t takes the coordinated system the current time, its

independence in various softwares entity. It avoided time not the synchronism. Increasing the time boundedness to the data actuation coordinated model makes it utilize in more open systems safely. For example applies it in Web Services can solve a service binding to enjoy permanently the service the limitation.

Mix key authentication mechanism(Ru-Chuan,2002) is the union of symmetrical key and the asymmetrical key which are two kind of coexisting authentication mechanisms, the correspondence entity consults its conversation key as well as in the key distribution center depositing correspondence entity registration information through the asymmetrical password system and the key distribution center and so on, but corresponds between the entity to authenticate the bilateral status through the symmetrical password system. This article utilizes this authentication way to the sharing tuple data space in the access control, read data from sharing space for the first time by asymmetrical key authentication, once through the status authentication, the system will establish a secret channel to transmit data with the software entity, it avoided the complex decipher computation through this secret channel transmission data. Utilizing mix the key authentication mechanism in the data actuation coordination model can reduce the system the computation order of complexity, simultaneously will increase the system the dynamic. Its authentication flow as shown in Figure 1.

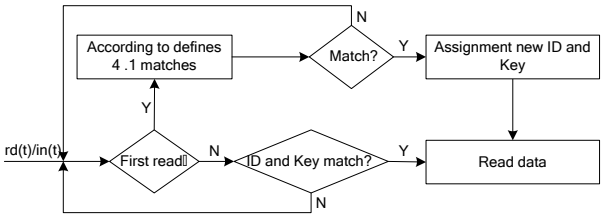

Fig.1 The Web of System Performance.

Security data actuation coordination model with the time restraint proposed not differentiate three kind of typical operations, simultaneously has the effectiveness boundedness to the data read operation, whicg guaranteed the coordinated system security.

5. Conclusion

This article proposes one kind of security data actuation coordination model with time restraint on foundation of analysis of the KLAIM, SecSOS, SecSpaces to, which could guarantee the communications security between the software entity. R. Lucchi and G. Zavattaro proposed WSSecSpaces(Lucchi,2004) (face Web Services application security data coordination service). The technology of coordinate applies to utilize for the first time in faces the service distributional technical Web Services. This article proposed the safe coordinated model also may take one kind of Web service form issued, exchange data between the service through the sharing tuple space,.It does not need the real-time communication between the service, simultaneously may control the service time through this model time boundedness, not only solved Web Services in the time and the spatial close coupling ,but also strengthens the service time control. But the model this article proposed has not carried on the control of writing data to the sharing space, namely any software entity all may write information to the sharing data space, which is a content will need to study future.

References

[1] R. De Nicola, G. Ferrari and R. Pugliese, “KLAIM: A Kernel Language for Agents Interaction and Mobility,”IEEE Transactions on Software Engineering,Vol.24(5),pp.315–330,1998.

[2] J. Vitek,C. Bryce and M. Oriol, “Coordinating Processes with Secure Spaces,”Science of Computer Programming,Vol.46(1-2),pp.163-193,2003.

[3] N. Busi,R. Gorrieri,R. Lucchi and G. Zavattaro, “Secspaces: a data-driven coordination model for environments open to untrusted agents,”Electronic Notes in Theoretical Computer Scienc,Vol.68(3),pp.310-327,2003.

[4] D. Gelernter,“Generative Communication in Linda,” ACM Transactions on Programming Languages and Systems (TOPLAS),Vol.7(1),pp.80–112,1985.

[5] W. Ru-Chuan,W. Shao-Di,S. Zhi-Xin and F. Jing, “Mix password authentication model research,”Chinese Journal of Computer,Vol.25(11),pp.1144-1148,2002(in Chinese).

[6] R. Lucchi and G. Zavattaro, “WSSecSpaces: a Secure Data-Driven Coordination Service for Web Services Applications,”Proceedings of the ACM Symposium on Applied Computing,Vol.1(1),pp.487-491,2004.