Distributed Certificates Chain Searching Algorithms Based on Trustworthy

Jianyun Lei and Yanhong Li*
School of Computer Science, South-Central University for Nationalities, Wuhan, China
*Corresponding Author, Email: leijianyun@mail.scuec.edu.cn, anddylee@163.com

Abstract—To address the distributed certificates searching problem in trust management, the member set and privilege set are defined, the forward, backward and bidirectional distributed certificates searching algorithms based on the definitions are brought forward, the complexity of the algorithms and also the comparison of the algorithms and existing algorithms are analyzed, the application of the algorithms is described with an instance. It is proved that the algorithm has high practicability and efficiency with the preprocess functions.

Index Terms—Access Control; Trust Management; Trustworthiness; Certificates Searching

I. INTRODUCTION

The certificates chain searching problem is a problem to find an authorized delegation chain from authorized source to access requester when the trust management system implements access control policy [1-3]. It is called centralized certificates chain searching problem if all the relevant certificates have been stored in local or a specific sites [4]. Ziqing Mao and his group brought forward an algorithm to address the certificates chain searching in SPKI/SDSI 2.0 system [5]. But because of the characteristics of distributed authorizing among every entity in the trust management system, certificates are generally distributed issued and stored, so the centralized certificates chain searching problem is derived to distributed certificates chain searching problem.

Distributed certificates chain searching algorithms are usually based on the centralized searching algorithms [6-8], but not all the centralized searching algorithms can be extended to the corresponding distributed searching algorithms. Centralized searching algorithms can be divided into bottom-to-up and up-to-bottom categories [9-12]. For an example, the algorithm given by Ziqing Mao in SPKI/SDSI 2.0 system is an algorithm of bottom-to-up [5]. It builds all legal certificates chains based on collection of certificates in local, and then search whether there exists desired certificates chain from all these certificates chains. Since many certificates are not stored in local in the distributed environments, it is not realistic to deduce based on all the certificates in the system [13-15]. While up-to-bottom algorithms can be easily extended to distributed algorithms [16]. It does the relevant certificates searching from a specific target (entity, role or certificate) as the starting point. For an example, aim at a role, search the certificates that define the role in the system, and then according to the entity in the certificates, to get new target and repeat this procedure to do the search. It’s not necessary to store all the certificates together like in the centralized algorithm. It only needs to provide the corresponding target to find those related certificates [17, 18].

Many algorithms have been brought forward to support distributed certificates chain searching in trust management systems, but most of these trust management systems require the certificates stored by the issuer, this will bring bottleneck in performance [19-22]. To design a searching algorithm of the distributed certificates chain, it is required to design the distributed storage solutions of certificates, that is who are responsible for the certificates storage.

Assume that certificate C is responsible by the entity S, when you find who is S, you can easily find the certificate C. The entity S is not compulsory to store certificate directly. It can be another entity on behalf of S to implement the specific certificate storage, such as a Lightweight Directory Access Protocol directory (LDAP) [23], and so on.

Generally, a certificate contains fields of issuer and subject, so the certificates can be stored either by the issuer or by the subject, therefore, the distributed storage program of the certificates can be divided into three categories [24]:

1) Certificates stored by the subject
2) Certificates stored by the issuer
3) Certificates stored partly by the subject and partly by the issuer, or implement the storage together by the two.

In the implementation process of the three above programs, only the access control lists are stored locally, while the details of the certificates’ storage location can be ignored in a distributed system, because the corresponding algorithm only has to find relevant or irrelevant collection of certificates that stored distributed.

Increase the trustworthy concept in the trust management system [25-27], that is, a trust value of a subject on an object represents the corresponding authorization delegation, indicated with the triples (S, O, T), where S stands for the subject of the certificate and O represent the object of the certificate, T is the trust value of the certificate, which denotes S on O, the trust has a value of T. Triples (S, O, T) is marked as: $S \xrightarrow{\tau} O$. 

Specific calculation of the trust can be found in reference [25].

Local access control list entries are represented by triples (R, Q, T). In which R indicates permission, Q stands for the access requester. T is the threshold value of the trust, which requires that Q has the value of the trust more than T to gain the right R. Triples (R, Q, T) is marked as: \( R \xrightarrow{\text{TRQ}} Q \).

It should be noted that in the authorization delegation certificate, subject S and object O are both probably the access requester Q in local access control list.

II. TRUSTWORTHY BASED DISTRIBUTED CERTIFICATES SEARCHING ALGORITHM

In order to find certificates chain quickly, firstly, certificates and local access control list in the system need a corresponding pretreatment. Add verify the validity of the certificates which is provided by access requester including: verify whether the certificates are expired, whether the trust value is in the scope of legal, and so on. The aim is to remove some of the excess options like cut the branch, and it will improve the efficiency of the certificates search algorithm.

To address the problem of certificates chain searching based on trustworthy in the distributed system, two definitions are given below.

**Definition 1** Suppose that there exists a collection of certificates (C), local access control list(L) and an access control permissions \( r \rangle \), then the collection is called the member set of the permissions \( r \rangle \) on the certificate set C and the local access control list L, denoted by M(r). The collection is consisted of all entities who owned access control permissions \( r \rangle \) in the system.

The solving process of finding M(r) is a cyclic solution. If the intermediate results which each loop obtained are marked as M\( r \rangle \), then the member set of permissions \( r \rangle \) contains the intermediate results and the new elements (members) who are authorized by the members in the set currently. So M\( r \rangle \)=[Q\( r \rangle (R, Q, T) \in L \cap R \supseteq r \rangle \], that is the member set which directly owns permission \( r \rangle \), M\( r \rangle \)=M\( r \rangle \)∪\{O\( (S, O, T) \in C \cap S \in M(r) \}\}. When M\( r \rangle \) and M\( r \rangle \) are equal, which indicate there is no new member authorized. Terminate the solving process, the M\( r \rangle \) or M\( r \rangle \) is the requested member set M(r).

**Definition 2** Suppose that there exists a collection of certificates (C), local access control list (L) and an entity (E), then all the privileges of entity(E) in the system form a set of privilege marked as P(E).

The solving process of finding P(E) is also a cyclic solution. If the obtained intermediate results are denoted as A\( E \), collection A used to represents the set which contain E and also the collection which direct or indirect authorize to E, then A\( E \)=A\( E \)∪\{S\( (S, O, T) \in C \cap O \in A\( E \)\} , this indicate P(E) contains the privilege that E owns and also the privilege that directly or indirectly authorized to E. When A\( E \)=A\( E \), which indicate there is no new authorization is delegated to the entity E, then terminate the solution process, \( [R \mid (R, Q, T) \in L \cap Q \in A\( r+1 \) (E)] \) is just the desired P(E).

Certificates chain searching algorithms consists of forward searching algorithm, backward searching algorithm and bi-directional searching algorithm. Correspond to start with a point of privilege to find the member set, start with a point of entity to find the privilege set and bi-directional matching algorithms.

A. Forward Searching Algorithm

The basic idea of the forward searching algorithm is to search a certificates chain from the permissions in the local access control list as a starting point. Known from definition 1, as long as the access requester is one of the element in M\( r \rangle \), it can be proved that it has the certificates chain, otherwise, there is no corresponding certificates chain.

Suppose the minimum permissions that visitor U need is \( r \rangle \). The description of the forward searching algorithm is as follow:

1. To find and calculate M\( r \rangle \) in the local access control list. M\( r \rangle \)=\{Q\( (R, Q, T) \in L \cap R \supseteq r \rangle \}. If M\( r \rangle \) is an empty set, there is no certificates chain can prove the access requester U has the permissions \( r \rangle \), and the end of the calculation is met. If the visitor U is an element in M\( r \rangle \), the access control entry (R, U, T) in the local access control list constitutes a certificates chain which proves U has the permission \( r \rangle \).

2. If U in (1) is not one element of M\( r \rangle \) and M\( r \rangle \) is not an empty set. According to the definition 1, to do the loop to calculate M\( i \rangle \) (\( i \geq 2 \)). M\( r \rangle \)=M\( i \rangle \)∪\{O\( (S, O, T) \in C \cap S \in M(r) \}\}. In the meantime, in order to avoid repeating the searching have done, the certificates and the intermediate results, the elements of M\( r \rangle \) are required to indexed, and the contact between certificates (Remember it's last certificate entry) are also required to recorded so as to construct the certificates chain. If the access requester U is one element of M\( r \rangle \), go to step (3); If the visitor U is not a member of Mi \( r \rangle \) and Mi \( r \rangle \) is equal to Mi-1 \( r \rangle \), then there exist no certificates chain, the calculation is ended.

3. It could be proved that access requester U has the certificates chain with the privilege \( r \rangle \). According to the link between the record certificates, construct the corresponding certificates chain.

B. Backward Searching Algorithm

The basic idea of backward searching algorithm is to search the certificates chain from a delegation subject as a starting point. Known from definition 2, if the access request is one of the element of P(E). It can be proved that there exists the certificates chain, otherwise, there is no corresponding certificates chain.

To find the set of privileges of U, the set contains privileges of U itself, and also the direct or indirect delegated permissions to U by other subjects. Collection A is used to indicate the set which contains U and also the collection which direct or indirect authorize to E by other subjects. Suppose the minimum permissions that
visitor U need is r. The description of the backward searching algorithm is as follow:

Do the Loops to calculate $A_i(U) \cap \{r\}, A_i(U) = \{U\}$, $A_{i+1}(U) = A_i(U) \cup \{S|(S,O,T) \in C \land O \in A_i(U)\}$ until $A_{i+1}(U) = A_i(U)$. In order to avoid the repeating the search, the certificates and the intermediate results are required to indexed. The elements of $A_i(U)$ and the contact between certificates are also required to recorded.

Calculate the privilege set $P(U)$. $P(U) = \{R|(R,Q,T) \in L \land R \supseteq r\}, A_i(U)$ if $M_{i+1}(r)=M_i(r)$, $A_{i+1}(U)$ can be found, or there exists no corresponding certificates chain.

If it can be proved access requester U has the certificates chain of the privileges r. According to the link between the recorded certificates, construct the corresponding certificates chain.

C. Bi-Directional Searching Algorithm

The basic idea of bi-directional search algorithm is to use both the forward searching method and backward searching method to search certificates chain at the same time. In the searching process, the judgment will be done once at each cycle whether the middle results of the forward searching algorithm and backward searching algorithm contain the same element, if it is, there is the access requester who has the privileges of the certificates chain, according to middle results to construct the corresponding certificates chain, otherwise, there is no corresponding certificates chain.

Suppose the minimum permissions that visitor U need is r. The bi-directional search algorithm is described as follow:

1. Search local access control list, calculate $M_1(r)$ $A_1(U)$, $M_1(r)=\{Q|(R,Q,T) \in L \land R \supseteq r\}, A_1(U)=\{U\}$, if $M_1(r)$ is null, there is no certificates chain that prove the access requester U has the privileges r, the algorithm exits. If $M_1(r) \cap A_1(U) \neq \emptyset$, the certificates chain has been found which prove the access request U has privileges r, the certificates chain is the local access control entry (R, U, T).

2. Do loop to calculate $M_i(r)$, $A_i(U)$ ($i>1$), the calculation ways of $M_i(r)$ and $A_i(U)$ are as same as in the forward searching algorithm and backward searching algorithm. If $M_i(r) \cap A_i(U) \neq \emptyset$, there exists the certificates chain which prove the access request U has privileges r, and go to step (3). If $M_{i+1}(r)=M_i(r)$, $A_{i+1}(U) = A_i(U)$ and $M_i(r) \cap A_i(U) = \emptyset$, there is no corresponding certificates chain.

3. If U has privileges r, according to the link of the recorded among the certificates in the calculation process, construct the corresponding certificates chain.

III. ALGORITHMS ANALYSIS AND COMPARISON

Suppose that a certificate set C have N certificates, the time complexity of the above three certificates chain searching algorithms are all O (n^2). In addition, each certificate needs only a storage in the whole process of searching, so the space complexity of searching algorithms are O(n).

Compared with the proposed model of the trust management certificates chain searching algorithm by others, for example, Li Ninghui proposed the RT model including the certificates chain search algorithm [28]. Freudenthal and others proposed the dRBAC model [29], certificates chain search algorithms brought forward in this paper are based on trustworthy and there exist certain trust value among the entities. When access the resources, the trust value of the entity to the resources should direct or indirect greater than a threshold. Based on this premise, pre-process of the searching can be done, and those extra certificates can be deleted, the efficiency of the certificates searching is greatly improved.

IV. AN EXAMPLE

The local access control list of a system is shown in Table 1. The set C of relevant delegation is shown in Figure 1. Trust transfer are calculated using $f(t1,t2) = t1*r2 /100$, which was presented in reference [25].

The question is: In October 2011, can Tom have the permission of Right_1?

<table>
<thead>
<tr>
<th>Sequence number</th>
<th>Rights</th>
<th>Entity</th>
<th>Trust threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Right_1</td>
<td>Sailor</td>
<td>70</td>
</tr>
<tr>
<td>2</td>
<td>Right_1</td>
<td>Kasi</td>
<td>80</td>
</tr>
<tr>
<td>3</td>
<td>Right_1</td>
<td>Grace</td>
<td>75</td>
</tr>
<tr>
<td>4</td>
<td>Right_2</td>
<td>Sailor</td>
<td>70</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

(1) [Sailor→Kate with 80, 12/30/2011]
(2) [Kate→John with 70, 10/30/2011]
(3) [John→Tom with 80, 10/30/2011]
(4) [Kasi→Tom with 90, 12/30/2009]
(5) [Grace→Tom with 90, 11/30/2011]
(6) [Jim→Bob with 95, 11/30/2006]

Figure 1. The set C of relevant delegation

According to Table 1 and Figure 1 to implement the corresponding calculation, respectively use forward searching, backward searching and bi-directional searching algorithms. The first pre-processing delete 4 and 6 of delegation collection because these two delegation records are expired.

Using the forward searching algorithm, the results are shown as follow.

Starting from the permission Right_1 to find its set of members M: Sailor, Kasi, Grace. Then search delegation collection, in the first cyclic we can get a result, through Sailor→Kate, Kate→John and John→Tom, but because $80*70*80/1000$ is less than 70, so there is no certificates chain can built in the routine. Next, we may find Right_1 to Tom's certificates chain, Grace→Tom's trust value is 90 which is greater than 75, so successfully find the certificates chain, the algorithm finished and construct the certificates chain Grace→Tom.

Using the backward searching algorithm, the results are as follow:

Starting from the user Tom to find his privilege sets R, in this solution, A collection contains elements of Grace...
and also John, Kate, Sailor can be found, and then due to the third item of local access control list, the appropriate certificates chain is found, the algorithm terminates and constructs certificates chain Grace→Tom.

Using bi-directional searching algorithm, the results are as follow:

Respectively, starting from the permission Right_1 and user Tom, find the Right_1’s set of users and the permissions set of user Tom, just one loop, the Grace permissions on Right_1 and delegation of Grace→Tom can be found, and then find the appropriate certificates chain, the algorithm terminates and constructs Grace→Tom’s certificates chain.

It can be found, the efficiency of the bi-directional search algorithm is relatively high, the problems can be solved using just one loop, but its storage required is increased because it requires both the storage for the intermediate result of the member set of Right_1 and Tom’s privilege set.

V. CONCLUSION

In the distributed environments, the value of the trust between the entities are required to obtain from the trust assessment tools firstly, and then use the searching algorithms based on trustworthy, through the judgment of trust between entities to selectively implement the searching of the appropriate certificates chain to improve the efficiency. In this paper, the member set of a privilege and also the privilege set of an entity are defined in the searching process in distributed environments. These definitions have a certain theoretical value. The paper also gives forward, backward and bi-directional distributed certificates chain searching algorithm based on trustworthy.

ACKNOWLEDGEMENT

This work was supported by the Natural Science Foundation of Hubei Province, China (No. 2013CFB445).

REFERENCES


[5] Ziqing Mao, etc. Distributed Credential Chain Discovery in Trust Management with Parameterized Roles and Constraints. Lecture Notes in Computer science, 2006, pp. 159-173


Jianyun Lei, born in September, 1972, in Zhejiang province, China, received the B.E degree in computer and application from South-Central University for Nationalities (SCUFN) in 1994, the M.S degree in computer software and theory from Huazhong University of Science and Technology (HUST) in 2004, and the Ph.D. degree in information security from Huazhong University of Science and Technology (HUST) in 2010.

Since 1994, he has been a faculty in South-Central University for Nationalities (SCUFN) which is in Wuhan, China, and he is currently an Associate Professor in the school of computer science. His recent research interests include information security, internet of things (IOT) etc.

Dr Lei is the member of China Computer Federation (CCF).

Yanhong Li was born on 26 April 1973 in Hunan, China. received the B.E. degree in mechanical engineering from Central South University of China(CSU) in 1993, The M.S. degree in computer application from Chongqing University of China (CQU)in 2004, and the Ph.D degree in computer software and theory from Huazhong University of Science and Technology of China (HUST) in 2011.

Since 2012, she has been a faculty in South Central University for Nationalities (SCUFN) which is in Wuhan, China, and she is currently a lecturer in the school of computer science. Her research interests include information security and multimedia network communication technology.