Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(3):703-707

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

Based on improved CAN PKI trust model

Hong Xiang Gong, Zhu Wen Hui, Liu Hao and Lv Xiang Yang

Nanchang University, China

ABSTRACT

PKI technology is the key to address some problems on interoperability of different PKI architecture and efficiently build certification paths. By analyzing several existing PKI trust model, this paper proposes a new PKI trust model that based on an improved CAN resource locating model. The new trust model can achieve safer, more effective cross domain authentication. The paper focuses on the number of possible routes between domains, and the time required for path construction.

Key words: PKI; Trust model; CAN; Path Construction

INTRODUCTION

With the continuously development of Internet and e-commerce, security certification becoming very important. Existing certification systems are primarily based on PKI (Public Key Infrastructure). And in X.509 [1] PKI, PKI is the use of public key cryptography to provide a secure basis for platform technologies and specifications: PKI technology uses the public key certificate management, third party trusted by organizations - CA (Certificate Authority), the user's public key and user bundled together with other identifying information in the Internet, verify the user's identity. Before a certificate can be used, it must be validated. In order to validate such a chain of certificates or a certificate path between the target certificate and trust anchor, and every certificate of within that path must be checked. This process is referred to as certification path processing. All of the entities of a PKI is the formation of a separate trust domains. PKI trust within CA and CA, CA and the user entity formed between the structural compositions of PKI system, known as the PKI trust model. PKI trust model is the abstraction of the overall framework, which determines the different entities within the organizational structure of the most important issue, is to establish PKI. This is because the trust model used on the network determines the form of trust and confidence in the form of the risk posed to provide a trust relationship establishment and management framework; PKI trust relationship as a transmission system, trust model is crucial, It shows how the PKI in the trust was created, it allows the security infrastructure, and by the restrictions imposed by this structure to do more reasoning.

With the development of information and increasing demand of information sharing, research on a PKI trust model has great significance. that is, the reason is that it can achieve cross domain authentication

2 SEVERAL PKI TRUST MODEL

2.1 HIERARCHICAL TRUST MODEL

Hierarchical trust model [2], shown in Figure 1, like an upside down tree structure, root is the starting point of trust , that we all trusted root CA, that is to say root CA is trust anchor in this trust model. The top-down parts of the branches have a CA, the leaf node is the user. Root CA for the issuance of its certificate of direct descendants of the node, and intermediate CA certify the public keys of its direct descendants of the node. In this model, certificates are issued in only one direction, and a CA never certifies another CA "superior" to itself. All nodes of the model have to trust the root CA, and keep a root CA's public key certificate. Communication between any two users, in order to validate each other's public key certificate, must be achieved through the root CA. When need to add a trust domain, the root CA of new trust domain should be a direct descendant of original root CA or sub CA.

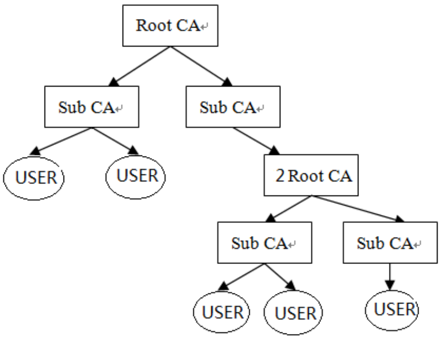

Figure 1. Hierarchical Trust Model

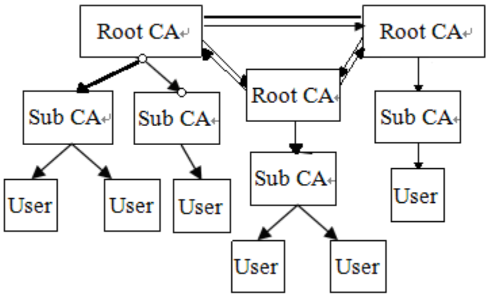

Figure 2. Hybrid Trust Model

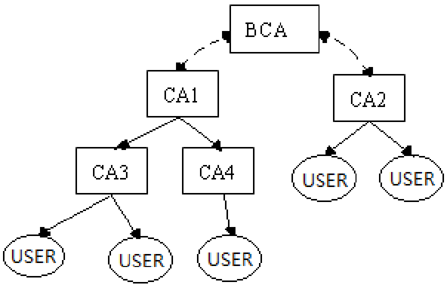

Figure 3. Bridge CA model

It can be seen in the hierarchical model, certification paths are easy to find because they are unidirectional and the longest path is equal to the depth of the tree less one, since root CA certificate is not part of the path. But in this trust model the root CA is the trust center for all users, if root CA trust crisis occurs, there is a crisis of confidence throughout the PKI system and the trust domain is not easy to scalable.

2.2 Hybrid Trust Model

In order to achieve interoperability between multiple trust domains, Hybrid Trust Model [2] is a combination of several trust models. For example, as shown in figure 2, every trust domain is a Hierarchical trust model, and all of root CA constitute a Mesh model [3] which means that every root CA has the digital certificate of the others. And users lies on each domain can verify each other. This model is easy to operate, widely used. But the management of cross-certificate becomes complicated with the trust domains of increasing.

3 BASED ON IMPROVED CAN PKI TRUST MODEL

3.1 improved CAN resource locating model

CAN (Content-Addressable Network) [4] resource locating model is applicable to large-scale dynamic network. The structure of CAN use of a virtual d-dimensional Cartesian coordinate space. The logical space is dynamically partitioned among all the nodes in the network, each node is responsible for one area of the space. In improved CAN[5] resource locating model, firstly ,nodes are divided into several groups that according to the physical location of the nodes. And each group like a small CAN called Group. Secondly, on the basis of the frequency of search Groups be divided into different grades of hot. Next use minimum cost path to achieve the resource location. A CAN node maintains a coordinate routing table that holds the IP address and virtual coordinate zone of each of its Neighbors and Group neighbors in the coordinate space. In a d-dimensional coordinate space, two nodes are neighbors if their coordinate spans overlap along d-1 dimensions and abut along one dimension. And two nodes are Group neighbors if two nodes are in a group and their coordinate spans overlap along d-1 dimensions and abut along one dimension. As shown in Figure 4, nodes are divided into Group A, Group B, Group C, Group D, then each group are divided into several teams. For example, Group A are partitioned into A1 to A9. When A1 need send a message to C8, First A1 uses CAN group routing mechanism and minimum cost path routing to A8.Then send the message to C8.

3.2 minimum cost path

Paths between two nodes in the dynamic system are not a single. The minimum cost path has the least routing delay between two nodes. Utilizing Shortest Path Faster Algorithm (Dijkstra) of weighted graph minimum cost path solved the problem of routing within group. Point and edge of weighted graph corresponds to node and neighbor node within a Group. If V0 and Vi are two nodes of a Group, the minimum cost path of V0 to Vi means in weighted graph which the weights is routing delay between nodes and its neighbor node within a Group use the Dijkstra algorithm to obtain the shortest path from V0 to Vi. Assume M is a set of some point in the weighted graph $G =< V, E >$, p is a path in G, a set $M' = V(G)\ M$, $dist(Vi, Vj)$ express the distance from Vi to Vj, in other word it is the summation of weights of the shortest path from Vi to Vj. And dist(Vi,M) express the distance from Vi to M means the minimum of $dist(Vi, Vm)$, and $Vm \in M$. Expression $w(Vi, Vj)$ means the weights of edge (Vi, Vj), when $i = j$,$w(Vi, Vj) = 0$,when Vi and Vj are not neighbors, $w(Vi, Vj) = \infty$. The following is the steps to obtain shortest path from V0 to Vk:

(1)set $M = \{V0\}$,then $dist(V0, M') = \min\{dist(V0, V) + w(V, U)\} = \min\{w(V0, U)\}$,in which $V \in M$, $U \in M'$ .Assume the path which satisfy the expression $dist(V0, M')$ is $p = (V0, Vi)$,next set $M = M + \{Vi\}$;

(2) Choose $p = (V0, \ldots, Vj)$,it makes $dist(V0, M') = \min\{dist(V0, V) + w(V, U)\}$,in which $V \in M$,$U \in M'$, next set $M = M + \{Vj\}$;

(3) Repeat step(2),until $p = (V0, \ldots, Vk)$.

Obtain minimum cost path in sequence from V0 to other nodes in Group, then we will get the minimum cost path table of V0. Within the group find a path according to the minimum cost path table of node , you can quickly locate the target node within the group.

3.3 Based on improved CAN PKI trust model

In PKI trust model, root CA which lies on different trust domains could be seen as a node, by obtaining digital certificate to identify each other information so that finish CA certification path construction, which is Similar to the process of resource locating. thus, this paper proposes a new Based on improved CAN PKI trust model. we mainly focus on the cross-domain situation, so this paper just discuss certification paths of root CA.

In the new trust model each root CA be seen as a node, these root CA are divided into several groups, such as Group A, Group B, Group C, Group D, Group E, and then each group also are divided into several teams in a virtual coordinate system. For example, Group A are partitioned into A1 to A5.

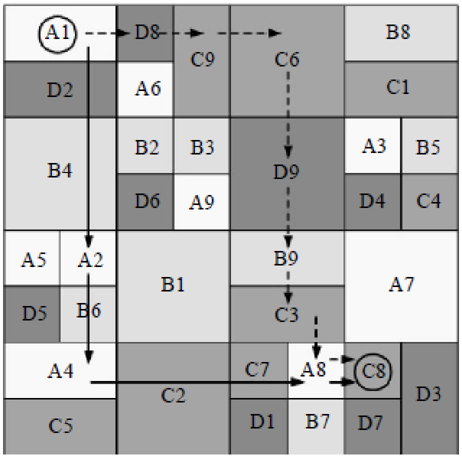

Figure 4. Improved CAN resource locating model

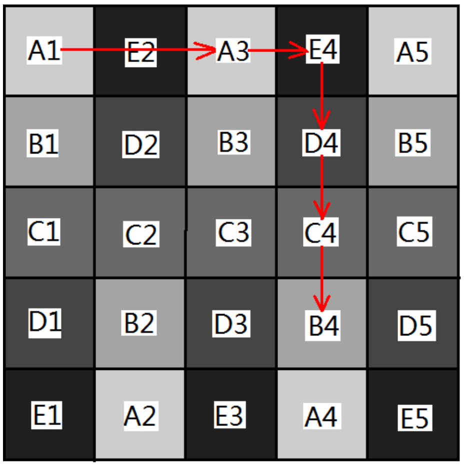

Figure 5. PKI trust model based on improved CAN resource locating model

Figure 5 shows, for the convenience of certificate management, every team is assigned one root CA, each node just have only one Neighbor in all directions. Every node with Neighbor or Group Neighbor are Cross-certification. And the digital certificate of root CA of Groups issued by the Group CA. For example, if A1 send a message to B4, first A1 uses CAN group certificate mechanism and minimum cost path routing to A3.Then A3 according to the coordinates of B4 to keep finding its Neighbor nodes until find B4.

3.4 Certificate path processing

The two end entities A and B, respectively, affiliate to CAi and CAj, the entire certification path algorithm described as:

Step1: B sends message and its certificate to A

B→A:$\mathrm{KB}-1(\mathrm{M}), \mathrm{CAj} << B >>$

Step2:A gets coordinate $(\mathrm{Xj}, \mathrm{Yj})$ from $\mathrm{CAj} << B >>$ and gets from Group CA we can know CAj from which group(GroupCAj),and gets its own coordinate $(\mathrm{Xi}, \mathrm{Yi})$ and GroupCAi. Then, go to step 3.

A:$\mathrm{CAj} << B >> | \rightarrow (\mathrm{Xj}, \mathrm{Yj})$、GroupCAj, $\mathrm{CAi} << A >> | \rightarrow (\mathrm{Xi}, \mathrm{Yi})$、GroupCAi

Step3:Along the direction of Xi to Xj query CAt,neighbors of $\mathrm{CAi} << A >>$, within the GroupCAi, if Xt between Xj and Xi replay Step3. If CAt abscissa meet $\mathrm{Xt}=\mathrm{Xj}$, when $\mathrm{Yt}=\mathrm{Yj}$ and CAt equals CAj,algorithm is over;when Yt not equal Yj, let$\mathrm{Yi}=\mathrm{Yt}$and go to Step4.Else let $\mathrm{Xi}=\mathrm{Xt}$ and go to Step6.

A:$\mathrm{R}(\mathrm{CAi} << A >>, XiXj) \rightarrow CAt, C(Xt, Xj)$

Step4: Along the direction of Yi to Yj query CAm,neighbors of $\mathrm{CAi} << A >>$, within the GroupCAi, if CAm's ordinate meet $\mathrm{Ym}=\mathrm{Yj}$ and CAm equals CAj algorithm is over;if Ym between Yj and Yj, let $\mathrm{Yi}=\mathrm{Ym}$ and replay Step4.Else let $\mathrm{Yi}=\mathrm{Ym}$ and go to Step5.

A:$\mathrm{R}(\mathrm{CAi} << A >>, YiYj) \rightarrow CAm, C(Ym, Yj)$

Step5: Along the direction of Yi to Yj query CAn , neighbors of $\mathrm{CAi} << A >>$, if CAn equals CAj algorithm is over. Else let $\mathrm{Yi}=\mathrm{Yn}$ and go to replay.

A:$\mathrm{R}'(\mathrm{CAi} << A >>, YiYj) \rightarrow CAn, C(Yn, Yj)$

Step6: Along the direction of Xi to Xj query CAk, neighbors of $\mathrm{CAi} << A >>$, if Xt between Xj and Xi replay Step6. If $\mathrm{Xk}=\mathrm{Xj}$, when $\mathrm{Yk}=\mathrm{Yj}$ and CAk equals CAj algorithm is over; when Yk not equal Yj let $\mathrm{Yi}=\mathrm{Yk}$ and go to Step4.

A:$\mathrm{R}'(\mathrm{CAi} << A >>, XiXj) \rightarrow CAk, C(Xk, Xj)$

4 PERFORMANCE ANALYSIS

Currently PKI trust models mostly are based on Hierarchical trust model and Mesh model, and in a Hybrid trust model all of root CA constitute a Mesh model. Therefore, select a hierarchical trust model which both deep and depth are 3 and hybrid trust model compared with the new model.

In large-scale trust domains, at best, the chain of certificates, according to the algorithm presented in this paper, Hierarchical trust model only needs 2. The algorithmic complexity can be expressed as $\mathrm{O}(2)$ [6]. while Hybrid trust model and based on improved CAN PKI trust model both are $\mathrm{O}(2)$. at worst, the algorithmic complexity of Hierarchical trust model is $\mathrm{O}(2\mathrm{n}+1)$, the Hybrid trust model is $\mathrm{O}(\mathrm{n})$,and the new trust model is $\mathrm{O}(\mathrm{n}/2+1)$. Therefore, the average algorithmic complexity of Hierarchical trust model is $\mathrm{O}(\mathrm{n}+3/2)$, Hybrid is $\mathrm{O}(\mathrm{n}/2+1)$ and new trust model is $\mathrm{O}(\mathrm{n}/4+1/2)$.

To further analyze the model performance, the paper make a performance test of three models by using java programming. In 10,25,40,80,100 trust domain test certification path length and time of certification path discovery process separately. Every case testing 1000 times shows in figure 6 and figure 7.

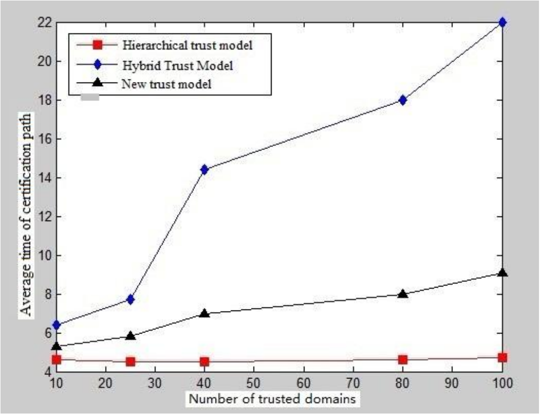

Figure 6.Average time of certification path in different domains

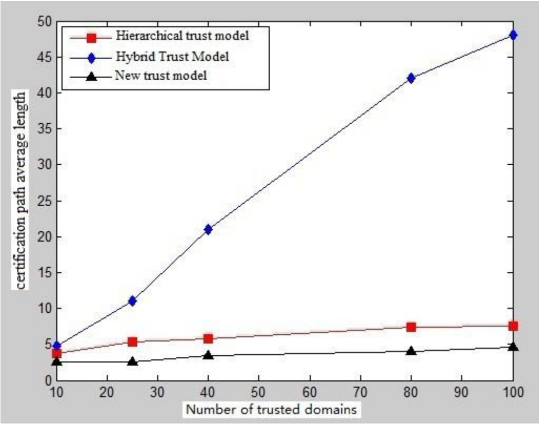

Figure 7. Certification path average length in different domains

Figure 6 shows the time of certification path of Hierarchical trust model is shortest and basically unchanged, and Hybrid trust model increase sharply,and the runtime of the path discovery process of Based on improved CAN PKI trust model just take a little time , compared with Hierarchical trust model with trust domain increasing.

Figure 7 shows certification path length of Hierarchical trust model and Based on improved CAN PKI trust model increase slowly, and Hybrid trust model increase sharply. while certification path length of Based on improved CAN PKI trust model is shortest with trust domain increasing.

In terms of security, Hierarchical trust model has only one trust anchor (root CA), once the root CA is attacked, the security of the entire network will be threatened. But the new trust model has more trust anchors and trust is dispersed in several roots CA. Even if parts of the root CA are attacked, the influence of the trust network is not obvious. So proposed improved CAN PKI trust model more secure.

CONCLUSION

Through the analysis of several PKI trust models, this paper propose a novel model--- based on improved CAN PKI trust model. Compared with Hierarchical trust model and Hybrid trust model, the new trust model has a shorter certification path length, a relatively short time of certification path and more secure. Therefore, it is more suitable for the communication between the large-scale trust domains. However, the new model still exists some shortcomes, for example, we can optimize group selection, model complexity for improve system performance.

REFERENCES

[1] ITU-T Recommendation X.509 (**2005**): Information Technology-Open Systems Interconnection - The Directory: AuthentiCAtion Framework[S], 08/05.
[2] Hou Liping and Shi Lei, "Research on Trust Model of PKI ", Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on Publications Date: 28-29 March **2011**.
[3] C. Satizabal, R. Paez, and J. Forne," PKI trust relationships: from a hybrid architecture to a hierarchical model", Availability, Reliability and Security, **2006**. ARES **2006**. The First International Conference on Publications Date: 20-22 April 2006.
[4] Sylvia Ratnasamy,Paul Francis,Mark Handley,et al.A scalable content-addressable network[C].San Diego,CA:Proceedings of the ACM SIGCOMM,**2001**:161-172.
[5] YU Weihua, XUE Bingbing and FAN Yihong. Improved strategy for CAN-based resource locating model [J]. Computer Engineering and Design, **2010**,(20).
[6] Changping Liu, Yong Feng, Mingyu Fan, Guangwei Wang,"PKI Mesh Trust Model Based on Trusted Computing", Young Computer Scientists, **2008**. ICYCS 2008. The 9th International Conference on Publications Date:18-21 Nov. **2008**.