2010 3rd International Conference on Computer and Electrical Engineering (ICCEE 2010)
IPCSIT vol. 53 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V53.No.1.26

Resources Access Control Strategy based on CPK Identification Authentication

Wen-Yuan Tang+, Qin-Wei Li and Mu Liu

College of Computer Science & Information Guizhou University, Guiyang, China

Abstract. Resource access control is a vital link to ensure the security of system. The combination of authentication and authorization is the guarantee of system security. A kind of resource access control scheme is proposed on the basis of CPK logo authentication system in this thesis. It generates an enormous amount of privilege assemble through the combination of small-scale authority seed access matrix. Then, it effectively combines authentication with access control making use of the new design resource access control protocol. It can ensure the system security under the premise of being no need to maintain a large number of data.

Keywords: Combination of public key; authenticate; privilege; authorization; mapped matrix

1. Introduction

With the developing of E-commerce, E-Government and E-Services, authenticating the trust relationship by digital method become significant. At present Public key infrastructure be widely used to authenticate all over the world.PKI has been widely applied in many fields, such as Grid Certification, Denied certification, decrypt, key management and so on . However, there are a lot of urgent problems need to be solved in implementation. An identification authentication system based on CPK algorithm be presented by XIANGHAO NAN who is one of the cryptogram experts in China. The system is based on reliable logical and implementing by CPK algorithm. A method of proving called "condition satisfy" be applied in CPK reliable logical. It includes four aspects—subject credibility, objects credibility, content credibility and action credibility. There is no doubt that it is a more advanced method than Formal reasoning to prove. So it became a solid foundation of constructing large and extensive credible certification system. The third party CA institutions no longer needed by the CPK system. Proving just by Shake hands on the net. It can be widely applied in mobile terminal such as cell phone. The supporting of LDAP is not necessary for certification process, ensuring its stability. The cost can be largely reduced, because the certification process is chip level. CPK certification system could be adopted in orderly network environment, such as bank, government, local tax and social insurance. With the deeply researching of CPK Identification Authentication, the resources access control Strategy based on the system also imminent.

2. The Principle of CPK

In view of ECC Scattering logarithm Take the resources less than other logarithms under identical safety condition. CPK key management mechanism is based on ECC scattering logarithm, and it take Elliptic curve group in finite field Fp(p is not equal to the prime number 2 and 3) to explain the mathematical principles and construction methods of CPK key Management Mechanism [8].

+ Corresponding author.
E-mail address: Tang-wy@163.com.

Combination of public key system is based on Elliptic Curve Cryptography in finite field P, and it define as (a, b, G, n, p). a and b constitute the cubic equation: $y^2 \equiv (x^3+ax+b) \bmod p$, G is the base point of additive group , n is the order of the group which based on G[1].

The composite theorem of ECC: in elliptic curve cryptography, the sum of public key equal to the sum of private key between all pairs of public and private keys. If the sum of private key is $(r_1+r_2+\cdots+r_m) \bmod n=r$, then the sum of public key is $R_1+R_2+\cdots+R_m= R$. so, r and R is a pair of key. Because $R = R_1+ R_2 + \cdots+ R_m= r_1G + r_2G + \cdots+ r_m G =(r_1+r_2+\cdots+r_m)G=rG$ [6].

CPK Identification Authentication applied to the trusted system, there are many advantages for the authentication, such as simple, easy, economic, efficient and traditional key management features. The most important thought is that it could generate a large number of keys by combining a small amount of matrix to resolve the problem of Large-scale key management. If the ECC parameters are known, the public(private) key matrix could be crate. The Public Key Seed Matrix (PSK):

$$\mathrm{PSK}=\begin{bmatrix} (x_{11,}y_{11}) & (x_{12},y_{12}) & \cdots & (x_{1h,}y_{1h}) \\ (x_{11,}y_{11}) & (x_{11,}y_{11}) & \cdots & (x_{11,}y_{11}) \\ \vdots & \vdots & \ddots & \vdots \\ (x_{11,}y_{11}) & (x_{11,}y_{11}) & \cdots & (x_{11,}y_{11}) \end{bmatrix}$$

The Private Key Seed Matrix (SSK):

$$\mathrm{SSK}=\begin{bmatrix} r_{11} & r_{12} & r_{13} & \cdots & r_{1h} \\ r_{21} & r_{22} & r_{23} & \cdots & r_{2h} \\ r_{31} & r_{32} & r_{33} & \cdots & r_{3h} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{m1} & r_{m2} & r_{m3} & \cdots & r_{mh} \end{bmatrix}$$

If the coordinate is definite—(i_1,j_1), (i_2,j_2), (i_3,j_3), (i_4,j_4), ⋯, (i_t,j_t). So the public key $PK=(x_{i1,y1}, y_{i1,j1})+(x_{i2,y2}, y_{i2,j2})+ (x_{i3,y3}, y_{i3,j3})+ (x_{i4,y4}, y_{i4,j4})+ \cdots+ (x_{it,yt}, y_{it,jt})$ and $SK=(r_{i1,j1}+ r_{i2,j2}+ r_{i3,j3}+ r_{i4,j4}+\cdots+ r_{it,jt}) \bmod n$. Because of PK=SK×G, it can be seen from this that CPK Identification Authentication could applied to grid certification.

3. Studying and Designing on Priviledge Access Control Strategy

The supporting of online database is not needed for the process of verify, this is one advantage of CPK Identification Authentication. Object public key be got by matrix and identification-mapped algorithm are public, they were generally stored in USB Key, IC card and PCB. It is foundation of the access control strategy proposed in this paper. It meets the condition of authority flexibility, while not increase the quantity of workload on data.

3.1The analysis of resources access control strategy

Access control strategy is a top guide for access controlling and access Decision-making. At present, there are three main types of access control strategy—discretionary access control, mandatory access control and role-based access control.

a) discretionary access control(DAC)

Discretionary access control is also known as identity-based access control. The main thought is that: The privilege of object accessing could be granted to other subjects by its owner. And the action of granting is transition. Although, the strategy is flexible, management of privilege authority is complex and not security.

b) mandatory access control(MAC)

Mandatory access control is also known as rules-based access control. The main thought is that the subjects and objects be separated into different classes. The access controlling according to the level tags of the subjects and objects. Management easily is the advantage of the strategy, But flexibility and integrity of controlling is not enough.

c) role-based access control(RBAC)

Role-based access control was proposed since the 1990s, and gradually developing into a access control model owing prefect functions. Comparing with DAC and MAC, RBAC stands for a great progress of flexibility and particle size controlling, it gradually replace the traditional access control model. The main thought is that: the privilege of accessing is assigned to roles, and users in the system were assigned certain roles. Comparing with the users, roles are relatively stable. This system will reallocate the roles if user changed. The strategy will simplify the authentication process.

According to the analysis of strategies such as DAC, MAC and RBAC, this paper proposed a matrix-based access control strategy, which combines the advantages of them all. The privilege matrix could be worked out by mapped-function, and it makes the exact controlling of various resources accessing come true.

3.2 Agreement and the definition of identity

- *Definition 1:* $R=\begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1h} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2h} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3h} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mh} \end{bmatrix}$

R is the mapped matrix on privileges, x-coordinate means the number of resources and y-coordinate means the number of privileges. The privileges include five values: Top-secret-1, Confidential-2, Secret-3, Internal-4, Public-5.

- *Definition 2: KMC*

  KMC mans Certificate and Key Management Center, the center is responsible for key management and certificate management and user registration.

- *Definition 3: AMC*

  AMC means Authorization Management Center, the center store the information of privileges, such as the identification and mapped function of privileges. User request to the Resource Management Center get the matrix R_l of the privileges when access to the first resource. Then get the value of privileges by computing, the value is $r=[1\ 2\ 3\ 4\ 5]\ R_l[1\ 0\ 0\ 0\ \cdots 0]^{-1}$,finally, compared to r_l(the privilege of the resource). If $r_l>r$, user could access the resource; else, user can apply the higher authority from AMC.

- *Definition 4: RMC*

  RMC means Resource Management Center, the center store all the information of the resources. Each resource acquire a pair of key(public key, private key, the privilege value) when register to the KMC.

- *Definition 5: CLIENT*

  CLIENT means the user. Each user acquire the private key, public key seed matrix, mapping algorithm of identification from RMC when access the resources.

3.3 privileges mapping

This mapping function is used with the user's privilege on the value of a collection of resources mapped to matrix of privilege, assuming there are n resources and five privilege values, the size of matrix R is n×5, the size of a small "matrix" by "portfolio" of generating extremely large number of privilege sets (5^n).

User's rights set were initialized by KMC when Registration, the staffs of management center authorizing through the mapping function of authorization system based on the user's permission information stored in the authorization management center. Resource Registry has been automatically granted in the minimum access of registered users, so matrix R and mapping functions are dynamic. Users could apply to authorization system to modify the privilege before access to the resources, staff of AMC authorized users after authenticated.

3.4 Agreements and processes of Resources Access

1) *CLIENT→RMC*： $D_1, [R_1, ID_{U\text{-}KEY}]SK_{U\text{-}KEY}$
2) *RMC→AMC*： i, D_2， $ID_{U\text{-}KEY}, \{[R_1, ID_{U\text{-}KEY}]SK_{U\text{-}KEY}], ID^1{}_{U\text{-}KEY}\}\ SK'_{U\text{-}KEY}$

3) *AMC→RMC：D_3 ，[R_2, r_i] $SK''_{U\text{-}KEY}$*

4) *RMC→CLIENT: IsPermit*

Explanation:

1) Users signature to the identity, requested information with their private key when access to the resources, then send the signature information, log request information to RMC. [R_1, $ID_{U\text{-}KEY}$]$SK_{U\text{-}KEY}$ is that encrypt the information of R_1 and $ID_{U\text{-}KEY}$ with the private key from U-KEY.

2) RMC get the identification(ID) and public key with D_1, PSK and mapping algorithm, then require $ID_{U\text{-}KEY}$ according to the signature information. If ID= $ID_{U\text{-}KEY}$, RMC encrypt the information of [R_1, $ID_{U\text{-}KEY}$]$SK_{U\text{-}KEY}$ with the private key $SK'_{U\text{-}KEY}$. Finally, RMC send the number of resource, $ID_{U\text{-}KEY}$ and signature information to AMC.

3) AMC get the public key of user and resource with their identification, then authenticate it with signature information, if the signature information is qualified, AMC acquire the value of privilege with the number of resource and identification of users. Finally, AMC signature to the value and send it to RMC.

4) RMC authenticate the signature information which from AMC, if the signature information is qualified, RMC will allow users to access the resources.

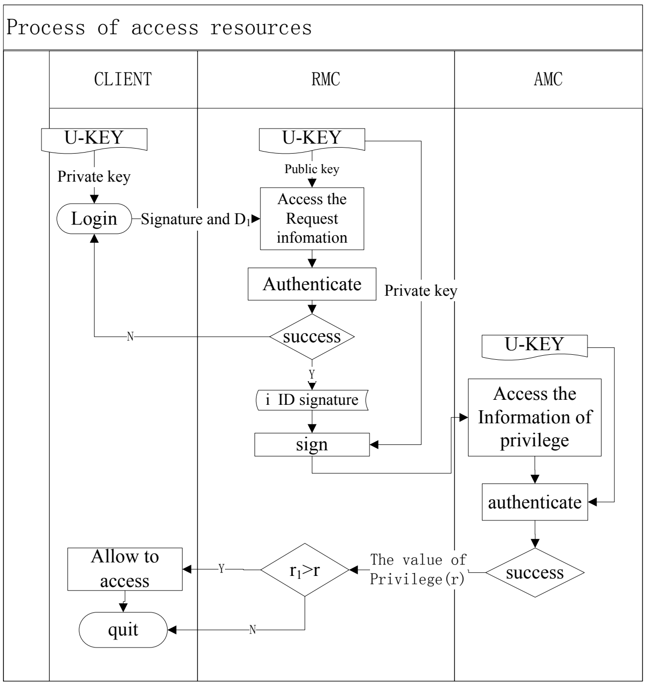

Figure1. Process of access resources

4. Conclusion

The resource access control scheme of research in this thesis has three primary advantages. Firstly, the authority assemble is achieved by the authority seed matrix through combination, so it does not need to maintain the large amounts of data. Secondly, design the new resource access protocol in order to dynamically combine access with authentication in applications. Finally, there also are differences in partition of isomerized resource permissions. The access control scheme in the design of this thesis take into consideration the compatibility of different resources.

5. References

[1] Huaping Chen.The Principle of Identity-based Combined Public Key System[J]. Computer Security, 2006, 6(2): 39-43.

[2] Xianghao Nan. Algorithm of Combined public key and Identification Authentication [J]. Information Security and Confidential Communication, 2006, 28(9): 12-16.

[3] Xianghao Nan. Certification of Identity-based Combined public key system [M]. BeiJing: National defense industry Press, 2006.

[4] Chenwei Gu. Analyse the defect of PKI and Prospect the new PKI[J]. COMPUTER AND DIGITAL PROJECT, 2006, 34(6): 55-57.

[5] Ellison C, Schneier B. Ten Risks of PKI[J]. Computer Security Journal, v 16, n 1, 2000, pp. 1-7.

[6] Chaohui Wang. The Security Research of ECC[D]. WuHan：WUHAN UNIVERSITY, 2004.

[7] Martinez G, Avila V S, Garcia C E, et al. Elliptic Curve Cryptography: Java Implementation Issues[C]//Proc. of IEEE International Carnahan Conference on Security Technology. Gran Canaria, Spain: [s. n.], 2005: 238-241.

[8] Wei Wan，Jindong Wang，HengWei Zhang.A Transfer Protocol of Identity-based Combined Public Key[J]. ZhengZhou:THE PLU INFORMATION ENGINEERING UNIVERSITY,201