Research on Authentication Method for Virtual Desktop System based on CPK

Ju Lei
Department of Communications Engineering
Beijing Electronic and Science Technology Institute
Beijing, China
e-mail: julei2000@163.com

Liu QiaoYu
School of Telecommunications Engineering
XIDIAN University
Xian, China
e-mail: qiaoyuliu@126.com

Chi YaPing
Department of Communications Engineering
Beijing Electronic and Science Technology Institute
Beijing, China
e-mail: chiyp_besti@163.com

***Abstract*—Virtual desktop technology separates the users and the resources, contributing to terminal security solutions and improvement of resource utilization. It also provides the convenience for the centralized management of resources. But the introduction of virtualization technology also makes unique safety risks existing in virtual desktop. Identity authentication is the key technology to solve the problem of virtual desktop security problems and also is the foundation of more complex security protective measures. This article first describes the principle of the Combined Public Key (CPK) cryptosystems, then according to the characteristics of the virtual desktop, two authentication methods based on CPK are proposed for virtual resources applying and virtual resources using respectively. And the user and the virtual machine is bound through the federated identity in order to prevent fraudulent use of virtual machine,. At last, the safety and performance analysis of the proposed authentication method is given.**

Keywords- Virtual Desktop; Identity authentication; Combined public key; Federated identity

I. INTRODUCTION

Virtual desktop which can completely separate the user and data is convenient for the centralized management to user's system, application and data. With increased resource utilization rate, enhanced the continuity of business, reduce the pressure of terminal security risks, and many other advantages, so it is widely used in recent years. At the same time, its unique security risks also have gradually received attention. Due to the virtual desktop based on virtualization technology, multiple virtual machines share hardware resources, and therefore need to provide the corresponding security solution for user data isolation, virtual machine protection and data storage, etc [1-3].

Identity authentication which is one of the key technology to solve the virtual desktop security can ensure that users remote login and use their own virtual resources, manage user's data, at the same time, more complex and fine-grained protection measures can also be implemented the virtual desktop system based on identity authentication.

According to the characteristics of the virtual desktop, two authentication methods based on CPK was proposed for virtual resources applying and virtual resources using respectively in this article. And for resists the risk of fraudulent using virtual machine effectively, a method of binding of the user ID and the virtual machine UIID through the federated identity was given. At last, the safety and performance analysis of the proposed authentication method is given.

II. THE CONCEPT FOR CPK

Identity-based Combined Public Key cryptosystems (CPK) belongs to a finite field of the elliptic curve cryptogram, its theoretical basis is the ECC key compound theorem [4]. In CPK V2.0 and later versions, the generation of key pair is divided into two parts, identity key generation and key composite [5]. Literature [6] [7] compares the CPK and PKI, the literature [8] [9] discusses the application of CPK in identity authentication.

Identity key generates as following steps:

1) Construction of the combination matrix. Combination matrix is divided into private key matrix and public key matrix, the matrix size is 32×32. Private key matrix is constituted of the random number which mutually different and less than n (n is the order of the group which basis point is the additive group of the basis point G). Let the element of matrix elements is r_{ij}, the private key matrix is denoted by SSK.

$$SSK=\begin{pmatrix} r_{1,1} & \cdots & r_{1,32} \\ \vdots & \ddots & \vdots \\ r_{32,1} & \cdots & r_{32,32} \end{pmatrix} \tag{1}$$

Public key matrix is derived by the private key, namely $r_{ij}G=(x_{i,j},y_{i,j})=R_{i,j}$, public key matrix is denoted by PSK.

$$PSK=\begin{pmatrix} R_{1,1} & \cdots & R_{1,32} \\ \vdots & \ddots & \vdots \\ R_{32,1} & \cdots & R_{32,32} \end{pmatrix} \tag{2}$$

2) The mapping of identity to the matrix coordinates. The length of YS is 165 bits, and w_1, w_2, ... w_{32} is 5 bits string which determines the coordinates of matrix.

$$YS = HASH(ID) = w_0, w_1, w_2, ...w_{32} \quad (3)$$

3) The calculation of identity key combination. Identity key (isk) is calculated in KMC, assume that the *i*-th row coordinates is denoted by w_i, column coordinates is denoted by $(u+i) \bmod 32$. Identity keys for entity A is :

$$isk_A = \sum_{i=1}^{32} r[w_i, (u+i)_{32}] \bmod n \quad (4)$$

Public key calculation can be achieved by elliptic curve times point addition:

$$IPK_A = \sum_{i=1}^{32} R[w_i, (u+i)_{32}] \quad (5)$$

Key composite is based on second-order key combined mechanism. The first-order combined key is the composite of system key and identity key which is generated by the KMC for individuals, a first-order combined private key csk' is the composite of identity private key isk and system private key ssk, calculated by the KMC:

$$csk'_A = (isk_A + rsk'_A) \bmod n \quad (6)$$

Second-order combined key is the composite of first-order combined key and update key defined by individual, the second-order combined private key csk''_A is the composite of first-order combined private key csk'_A and updated private key usk'_A, calculated by the signer:

$$csk''_A = (csk_A + usk_A) \bmod n \quad (7)$$

Attendant public key is the composite of system public key and updates public key, calculated by the signer:

$$ASK''_A = SPK_A + UPK_A \quad (8)$$

Second-order combined public key is the composite of identity public key and attendant public key, calculated by the verifier:

$$CPK''_A = IPK_A + APK''_A \quad (9)$$

III. AUTHENTICATION FOR VIRTUAL RESOURCES APPLYING BASED ON CPK

For virtual desktop system, when registered users request virtual resource through the local terminal, virtual desktop server needs to authenticate the user and assign virtual resources to user that can be used. CPK key system can issues CPK public and private key for virtual desktop user centrally, and is responsible for key management. CPK public key can be obtained in two ways: one is from the system key table stored in online databases which providing inquiry and maintenance services; and another is from the system key table stored in the local media of user.

The identity authentication system based on CPK is divided into local registration management center and CPK key management center. CPK key management center contains internal certificate registration server, the key generation server, key management server and open database server. Certificate registration server verifies the users' identity, and distributes users' ID certificates. Key generation server and key management server generates the users' public and private key pair and certificate registration server distributes to users via offline or a secure channel. In order to reduce the server workload, each user can download the public key matrix of system to the local.

If let U for the user, the UID for users' ID, UIDC for user' ID certificate, LRMC for local registration management center, CRGS for certificate registration server, KGC for key generation center, KMC for key management center, the user U apply to the key management center for CPK public-private key pair process as shown in figure 1, the related description is as follows:

1) $U \to LRMC$: Request; U submits application for registration to LRMC;
2) $LRMC \to U : UID$; LRMC generate the UID which contain the user information and sent UID to the user;
3) $U \to CRGS : \mathrm{Re}\,quest \| UID$; U submits application to CRGS, CRGS review ID identity further;
4) $CRGS \to KGC : UID$; CRGS sends the users' UID to KGC;
5) $KGC : CPK'_U, csk'_U, KGC \to KMC : CPK'_U, csk'_U$; KGC generates a first-order combined key CPK'_U, csk'_U for user to, and send to KMC;
6) $KMC \to CRGS : CPK'_U, csk'_U$; KMC sends CPK'_U, csk'_U to CRGS;
7) $CRGS \to U : UIDC$; CRGS sends UIDC to U by the secure channel;
8) $U : CPK''_U, csk''_U$; U select update Key and compute Second-order combined key CPK''_U, csk''_U.

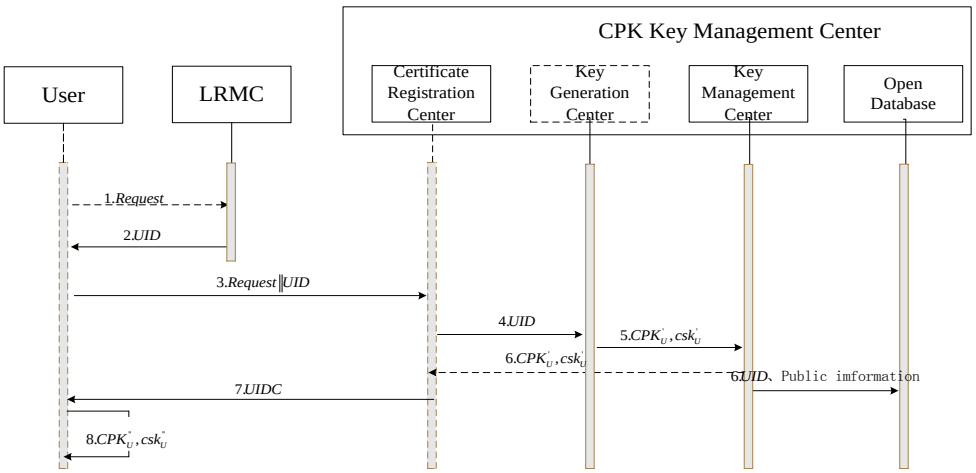

Figure 1. The processes of users apply for CPK key

The process of virtual desktop server authenticates the user's identity using CPK key system as follows:

1) $U: R = \{UID, ASK_U'', r\}$, $sign = E_{csk''}[Hash(R)]$; Where r is a random number;
2) $U \to S: R \| sign$; U requests S to log in virtual desktop system;
3) $S: CPK_U''$; According identify UID, S calculates Second-order combined key;
4) $S: sign^{-1} = E_{CPK_U''}[sign] = Hash'(R)$; S verifies the signature of U, if $Hash'(R) = Hash(R)$, the authentication succeeds, S provides virtual resources to U.

IV. AUTHENTICATION FOR VIRTUAL RESOURCES USING BASED ON CPK

In the using of virtual machines, users need to log in the virtual machine, and then use the virtual machines or access to external applications through virtual machines. To ensure that users can legally use the virtual resources assigned to them, the virtual machine need to authenticate users. And while the user using a virtual machine to access the external application, application providers also need to authenticate the user identity and even virtual machines to ensure that the authenticity of service object. To meet certification requirements in the using process of virtual machine, an authentication methods based on CPK was proposed for authenticate the user and virtual machines simultaneously. The system architecture which apply authenticate methods based on CPK is shown in Figure 2.

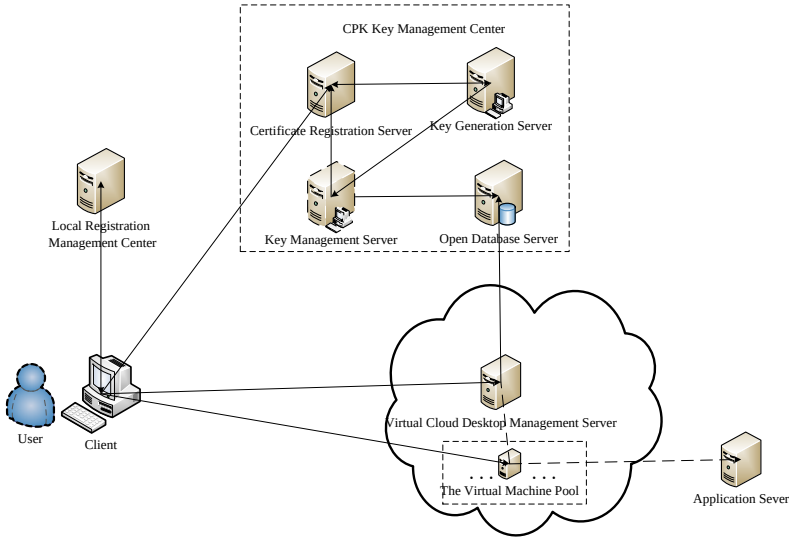

Figure 2. Architecture of CPK authenticate methods apply system

In figure 2, CPK key management center distributes CPK keys for authentication to the users of virtual desktop system. New users should apply to CPK key management center for ID certificate firstly. And after obtain the user ID certificate, users sent application to the virtual desktop management server and request to log in virtual desktop system. Virtual

desktop management server assigns a virtual machine to authenticated user, and then binds the virtual machine's serial number UIID and users' identity UID together. Let the federated identity formation as a virtual machine CPK key system identity VMID, and CPK key systems t generate ID certificate for virtual machines based on VMID.

Virtual machine for the user authentication process is as follows (the VM for the virtual machine, AS for the application server):

(1) $U: R = \{UID, ASK''_U, r\}, sign = E_{csk''}[Hash(R)]$

(2) $U \to VM: R \| sign$

(3) VM : user ID UID extracted from the R compare to the user ID binded in VMID, if equals, then continue;

(4) $VM: CPK''_U, sign^{-1} = E_{CPK''}[sign] = Hash'(R)$; VM calculates Second-order combined public key based on identity UID, if $Hash'(R) = Hash(R)$, the authentication succeeds. According to section III, it shows that the user U is the assigned user to virtual machines, so U can use virtual machines to access appropriate resources.

When user U uses a virtual machine VM to access to external application server, the application server authenticates user identity and virtual machine simultaneously. Because the identity of the virtual machine is federated identity VMID, binding relationship between the user and the virtual machine can be determine through certificates the virtual machine, and then combined with user authentication is able to effectively prevent fraudulent use of the virtual machine. Certification process is as follows:

1) $VM: R_d = \{VMID, ASK''_{VM}, r\}, SIGN = E_{csk''_{VM}}\left[Hash(R_d)\right]$

2) $VM \to AS: R_d \| R \| SIGN \| sign$;

3) $AS: CPK''_{VM}, SIGN^{-1} = E_{CPK''_{VM}}[SIGN] = Hash(R_d)$, $CPK''_U, sign^{-1} = E_{CPK''_U}[sign] = Hash'(R)$; Application server AS first extract the user ID from VMID and compares with UID, if the same, calculates Second-order combined public key of VM and U, respectively verifies the signatures of VM and U, if $Hash'(R_d) = Hash(R_d)$, $Hash'(R) = Hash(R)$, completes the VM and U certification.

V. Security and Performance Analysis

In terms of security, in the given method, the user ID and the virtual machine identity UIID are bound to a federated identity, enabling the user identity and the virtual machine identity binding together, so it can prevent the fraudulent after virtual machine being attacked effectively. In addition, all the authentication methods in the virtual cloud desktop system are based on CPK cryptosystem, based on the CPK's safety performances; the whole system has higher security.

From the practical point of view, for the proposed authentication methods based on the CPK is used by whole virtual desktop system, the unified management and maintenance can be achieved easily. And the CPK can achieve ultra-large-scale key distribution, and does not require third-party online participation, so it can meet the authentication needs of a large number of users and will not form a performance bottleneck. Authors and Affiliations

VI. Conclusion

In this article, to the specific security risks in virtual desktop, authentication methods are proposed under applying the virtual resources and using virtual resources two scenarios based on CPK, and specific authentication process is given. The safety and performance analysis of the proposed authentication method is given. Authentication is the basic information security technology, if combines t he proposed method with authentication and identity management, policy management, it is possible to design a more effective virtual desktop protection method. CPK itself features make the proposed method support a large amount of users' authentication requirements, but due to the user is bound with the virtual machine, this method is suitable for the occasions of stable users and fixed virtual resource allocation.

Acknowledgment

This work was supported in part by the Fundamental Research Funds for the Central Universities (YZDJ1202).

References

[1] Zhi-yong Zheng,Yuan-da Lv,Yi Wang. Virtual Deskpot System Analysis and Countermeasures. Network Security Technology and Application. 2012,10(10): 50-52

[2] Yu Sun,Yu-xin Chen. Desktop Virtualization and Security Technology Research. Information Security and Secrecy of Communication. 2012, 33(6):87-88,92

[3] Zhi Ning, Zheng Fang. Exploration about Classified Information System Virtualization Security. Secret Science and Technology. 2012,22(2):70-74

[4] Xiang-hao Nan. CPK Cryptosystem and the Security. Beijing: National Defence Industry Press. 2008

[5] Xiang-hao Nan. CPK Combined Public Key Cryptosystems（v8.0）. Information Security and Secrecy of Communication. 2013,34(3):39-44

[6] Jia-fa Zhou, Tao Ma, Yi-fa Li. PKI、CPK anf IBC Performance Analyses. Journal of Information Engineering University. 2005,6(3):26-31

[7] Jia-lin Wang. Contrastive Analysis to Large-scale Network Authentication Scheme based on PKI and the CPK. Secret Science and Technology.2012, 6:44-49

[8] Wei Tang. Cloud Security Research based on Combined Public Key Cryptosystems. Huazhong University of Science and Technology Master's Thesis. 2011,5

[9] Yu-chi Ma， Yuan Zhao， Yi-qun Deng. Trusted Platform User Login Authentication Scheme based on CPK. Computer Engineering and Application. 2010,46(1):90-94