

基于CPK的虚拟桌面系统认证方法研究

鞠磊¹ 池亚平¹ 刘巧瑜^{1,2} 封化民¹

(北京电子科技学院通信工程系 北京 100070)¹ (西安电子科技大学通信工程学院 西安 710071)²

摘要 虚拟桌面技术将用户与资源分离,有助于终端安全的解决和资源利用率的提高,也为资源的集中管理提供了便利,但虚拟化技术的引入也使得虚拟桌面存在其特有的安全隐患。身份认证是解决虚拟桌面安全问题的关键技术,也是实施更复杂和细粒度的安全防护措施的基础。首先介绍了组合公钥CPK的基本原理,然后针对虚拟桌面的特点,基于CPK给出了虚拟资源申请和虚拟资源应用两种场景下的身份认证方法,并通过联合标识实现了用户与虚拟资源的绑定,最后给出了所提方法的安全性和实用性分析。

关键词 虚拟桌面,身份认证,组合公钥,联合标识

中图分类号 TP393.08 文献标识码 A

Research on Virtual Desktop System Authentication Method Based on CPK

JU Lei¹ CHI Ya-ping¹ LIU Qiao-yu^{1,2} FENG Hua-min¹

(Department of Communications Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China)¹

(Department of Communications Engineering, Xidian University, Xi'an 710071, China)²

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 exist 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 and fine-grained security protective measures. This article first described the basic principle of the combined public key(CPK) cryptosystems, and then according to the characteristics of the virtual desktop, based on CPK authentication methods was proposed under applying the virtual resources and using virtual resources two scenarios. Through the federated identity, the binding of the user and the virtual machine comes true. At last, the safety and performance analysis of the proposed authentication method was given.

Keywords Virtual desktop, Identity authentication, Combined public key, Federated identity

1 引言

虚拟桌面能够实现用户和数据的完全分离,便于用户系统、应用和数据的集中管理,具有提高资源利用率、增强业务的连续性、减轻终端安全风险压力等诸多优点,因此近些年来得到了广泛应用,同时其特有的安全风险也逐渐受到了关注。由于虚拟桌面以虚拟化技术为基础,多个虚拟机会共享硬件资源,因此需要针对虚拟环境下的用户数据隔离、虚拟机防护、数据存储等方面提供相应的安全解决方法^[1-3]。身份认证是解决虚拟桌面安全问题的关键技术之一,通过对用户身份的确认,可以保证用户远程登录和使用自己的虚拟资源,管理用户的数据,同时虚拟桌面系统也可根据用户身份实施更复杂和细粒度的防护措施。

本文基于CPK组合密码体制给出了针对虚拟桌面的认证方法,分别针对虚拟资源申请和虚拟资源使用两种场景设计了认证协议,通过联合标识实现了用户与虚拟机的绑定,有效抵御了虚拟机的冒用风险,最后在安全与性能方面对所提

出的认证方法进行了分析。

2 组合公钥CPK简介

基于标识的组合公钥密码体制(CPK)属有限域上的椭圆曲线密码,其理论依据是ECC密钥复合定理^[4]。CPK组合公钥体制V2.0及其以后版本,将密钥的产生分为标识密钥产生及密钥复合两部分^[5]。文献^[6,7]对CPK与PKI进行了比较,文献^[8,9]则探讨了CPK在身份认证中的应用。

标识密钥按如下步骤产生:

(1)构建组合矩阵。组合矩阵分为私钥矩阵和公钥矩阵,矩阵大小均为 32×32 。私钥矩阵由互不相同的小于 n (n 为以加法群的基点 G 为基点的群的阶)的随机数构成,矩阵中的元素标记 $r_{i,j}$,私钥矩阵记为SSK。

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

公钥矩阵由私钥矩阵派生,即 $r_{ij}G = (x_{i,j}, y_{i,j}) = R_{i,j}$,公

本文受中央高校基本科研业务费(YZDJ1202)资助。

鞠磊(1971—),男,博士,讲师,主要研究方向为信息安全、云计算, E-mail: julei2000@163.com; 池亚平(1969—),女,教授,主要研究方向为信息安全; 刘巧瑜(1988—),女,硕士生,主要研究方向为信息安全; 封化民(1963—),男,博士,教授,主要研究方向为信息安全、多媒体智能处理。

钥矩阵记为 PSK 。

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

(2) 实现标识到矩阵坐标的映射。映射通过对标识的 HASH 变换实现,将 HASH 输出调整长度为 165bit 的映射序列 YS ,以 5bit 构成 $w_1, w_2, \dots, w_{32}$ 的字符串,用于决定列坐标与行坐标。

$$YS = HASH(ID) = w_0, w_1, w_2, \dots, w_{32}; (w_{33}, -w_{36}) \quad (3)$$

(3) 实现标识密钥的组合计算。标识密钥 (isk) 的计算在 KMC 中进行,设第 i 次行坐标用 w_i 表示,列坐标用 $(u+i) \bmod 32$ 表示。实体 A 的标识密钥为:

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

公钥计算以椭圆曲线 $Ep(a, b)$ 上的倍点加法实现,

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

密钥复合采用二阶复合的密钥机制。密钥的一阶复合是指由管理中心为个体生成一对一的系统密钥和标识密钥的复合,一阶复合私钥 csk_A' 是标识私钥 isk 和一阶系统私钥 ssk 的复合,由 KMC 计算:

$$csk_A' = (isk_A + rsk_A') \bmod n \quad (6)$$

密钥的二阶复合是一阶复合密钥和个体定义的更新密钥的复合,二阶组合私钥 csk_A'' 为一阶组合私钥 csk_A' 和更新私钥 usk_A 的复合,由签名方计算:

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

伴随公钥为系统公钥与更新公钥的复合,由签名方计算:

$$ASK_A'' = SPK_A' + UPK_A \quad (8)$$

二阶组合公钥为标识公钥与伴随公钥的复合,由验证方计算:

$$CPK_A'' = IPK_A + APK_A'' \quad (9)$$

KMC 负责密钥集中产生和管理以及私钥矩阵的保存,CPK 中的公钥公开,公钥矩阵放在用户最容易获得的地方以便查阅[4]。

3 基于 CPK 的虚拟资源申请认证方法

对于虚拟桌面系统,经过注册的用户通过本地终端向其申请虚拟资源时,虚拟桌面服务器需要对用户的身份进行认证,通过认证后才为其分配可使用的虚拟资源。CPK 密钥系统可为虚拟桌面用户集中发放 CPK 公私钥,并负责密钥的管理工作。CPK 公钥的获取方式有两种,一种是将系统密钥表存放于在线数据库中,对外提供查询服务,并随时维护;另一种是将系统密钥表存放于本机媒介中,在本地直接取用,定期维护。

基于 CPK 的身份认证系统分为本地注册管理中心和 CPK 密钥管理中心两部分。CPK 密钥管理中心内部包含证书注册服务器、密钥生成服务器、密钥管理服务器和公开数据库服务器。证书注册服务器对用户的标识进行验证,分发用户的 ID 证书。密钥生成服务器和密钥管理服务器生成用户的公私钥对,然后由证书注册服务器通过离线方式或安全通道发放给用户。对于整个系统的公钥矩阵,每个用户可下载到本地进行查阅,以减少服务器工作量。

若令 U 为用户,UID 为用户 U 的 ID,UIDC 为用户的 ID 证书,LRMC 为本地注册管理中心,CRGS 为证书注册中心,KGC 为密钥生成中心,KMC 为密钥管理中心,则用户 U 向密

钥管理中心申请 CPK 公私钥对的流程如图 1 所示,相关描述如下:

- 1) $U \rightarrow LRMC: Request$; 用户向本地的注册管理中心 LRMC 递交注册申请;
- 2) $LRMC \rightarrow U: UID$; 通过审核后生成一张含有用户信息内容的用户 ID 标识 UID 发送给用户;
- 3) $U \rightarrow CRGS: Request \parallel UID$; 用户向 CRGS 提出申请,CRGS 对标识进行进一步审核;
- 4) $CRGS \rightarrow KGC: UID$; CRGS 将用户 UID 发送给 KGC;
- 5) $KGC: CPK_U', csk_U'$, $KGC \rightarrow KMC: CPK_U', csk_U'$; KGC 为用户生成一阶复合密钥 CPK_U', csk_U' ,并发送给 KMC;
- 6) $KMC \rightarrow CRGS: CPK_U', csk_U'$;
- 7) $CRGS \rightarrow U: UIDC$; CRGS 将 UIDC 通过安全信道发送给用户 U ;
- 8) $U: CPK_U'', csk_U''$; 用户选择更新密钥计算二阶复合密钥 CPK_U'', csk_U'' 。

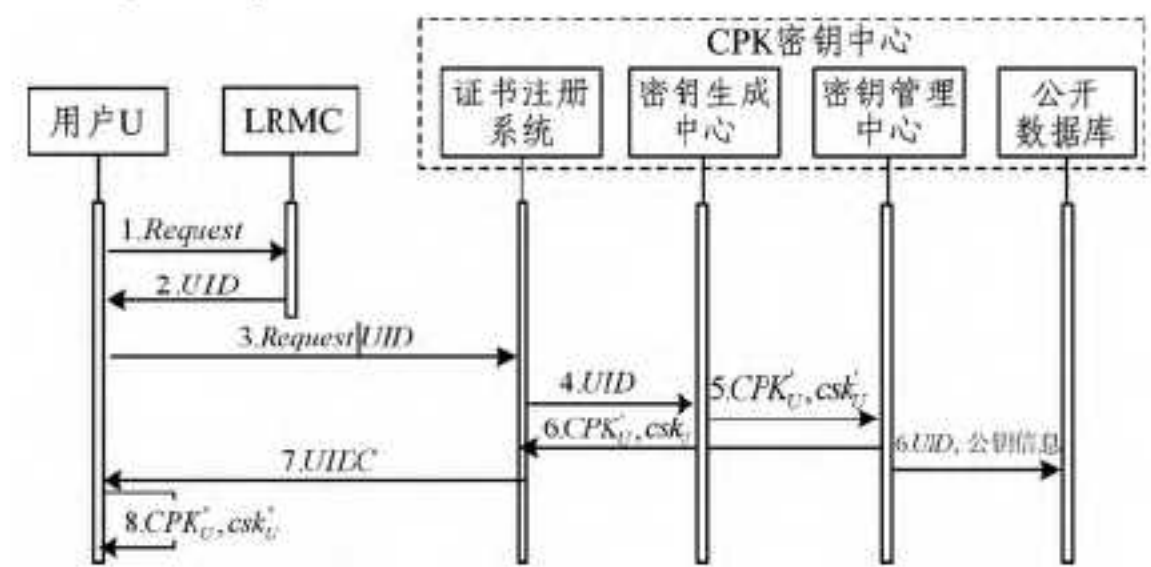


图 1 用户申请 CPK 密钥流程

虚拟桌面服务器利用 CPK 公钥系统对用户进行身份认证的具体流程如下:

- 1) $U: R = \{UID, ASK_U'', r\}$, $sign = E_{csk_U''}[Hash(R)]$; r 为随机数;
- 2) $U \rightarrow S: R \parallel sign$; U 向 S 请求登录云桌面系统;
- 3) $S: CPK_U''$; S 根据标识 UID 计算 U 的二阶复合公钥;
- 4) $S: sign^{-1} = E_{CPK_U''}[sign] = Hash'(R)$; S 对 U 的签名进行验证,若 $Hash'(R) = Hash(R)$,则认证通过, S 为 U 提供相应虚拟资源。

4 基于 CPK 的虚拟资源使用认证方法

用户在使用虚拟机时首先需要登录虚拟机,然后使用虚拟机或通过所使用虚拟机访问外部应用服务。为保证用户能够使用合法分配给其使用的虚拟资源,虚拟机在用户登录时需要对用户身份进行认证,而用户使用虚拟机访问外部应用时,应用提供方也需对用户身份甚至虚拟机进行认证,以保证服务对象的真实性。为满足虚拟机使用过程中的认证需求,设计了如下基于 CPK 的认证方法。基于 CPK 的虚拟桌面系统架构如图 2 所示。

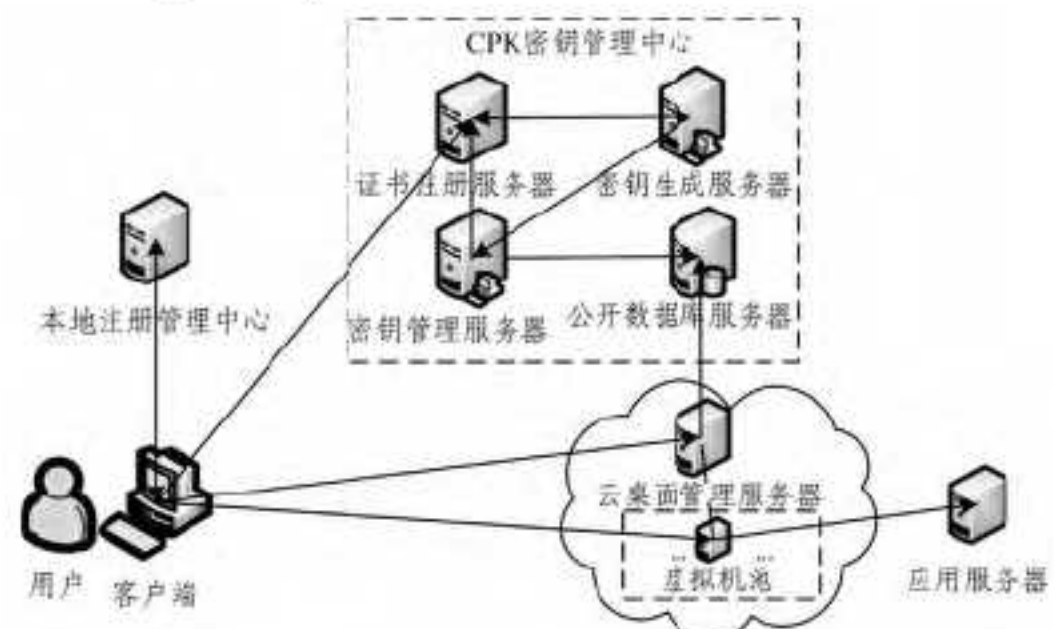


图 2 基于 CPK 的虚拟桌面系统架构

图2中,CPK 密钥管理中心为虚拟桌面系统的用户分发用于身份认证的CPK 密钥。第一次登录的用户应先在CPK 密钥管理中心申请获得ID 证书,获得ID 证书后用户向虚拟桌面管理服务器发送申请,请求登录虚拟桌面系统。虚拟桌面管理服务器为通过认证的用户分配虚拟机,然后将虚拟机序列号UIID 与用户标识UID 进行绑定,形成联合标识,并将其作为虚拟机的CPK 密钥系统的标识VMID,即 $VMID=UIID \parallel UID$,CPK 密钥系统根据VMID 为虚拟机生成ID 证书。

虚拟机对用户进行认证流程如下(VM 为虚拟机,AS 为应用服务器):

- 1) $U: R = \{UID, ASK_U'', r\}, sign = E_{cpk_U} [Hash(R)];$
- 2) $U \rightarrow VM: R \parallel sign;$
- 3) VM: 从 R 中提取用户标识UID,与VMID 中的绑定的用户标识进行比对,若相等,则继续;
- 4) $VM: CPK_U'', sign^{-1} = E_{CPK_U} [sign] = Hash'(R);$ VM 根据标识UID 计算 U 的二阶复合公钥,若 $Hash'(R) = Hash(R)$,VM 对 U 的注册身份认证通过。根据第3)步可知该用户 U 即为虚拟桌面服务器为本虚拟机分配的使用者,所以 U 可以使用虚拟机访问相应资源。

用户 U 利用虚拟机 VM 访问外部应用服务器时,应用服务器对用户身份和虚拟机同时进行认证,由于虚拟机的标识为联合标识VMID,通过对虚拟机的认证能够确定用户与虚拟机的绑定关系,再与用户身份认证相结合则能够有效防范虚拟机冒用问题。认证流程如下:

- 1) $VM: R_d = \{VMID, ASK_{VM}'', r\}, SIGN = E_{cpk_{VM}} [Hash(R_d)];$
- 2) $VM \rightarrow AS: R_d \parallel R \parallel SIGN \parallel sign;$
- 3) $AS: CPK_{VM}'', SIGN^{-1} = E_{CPK_{VM}} [SIGN] = Hash(R_d),$
 $CPK_U'', sign^{-1} = E_{CPK_U} [sign] = Hash'(R);$ 应用服务器AS 首先提取出VMID 中的用户标识与UID 进行比对,一致后计算VM 和 U 的二阶复合公钥,并对VM 和 U 的签名分别进行验证,若 $Hash'(R_d) = Hash(R_d), Hash'(R) = Hash(R)$,同时完成对VM 和 U 的认证。

整个虚拟资源使用过程中的认证流程如图3 所示。

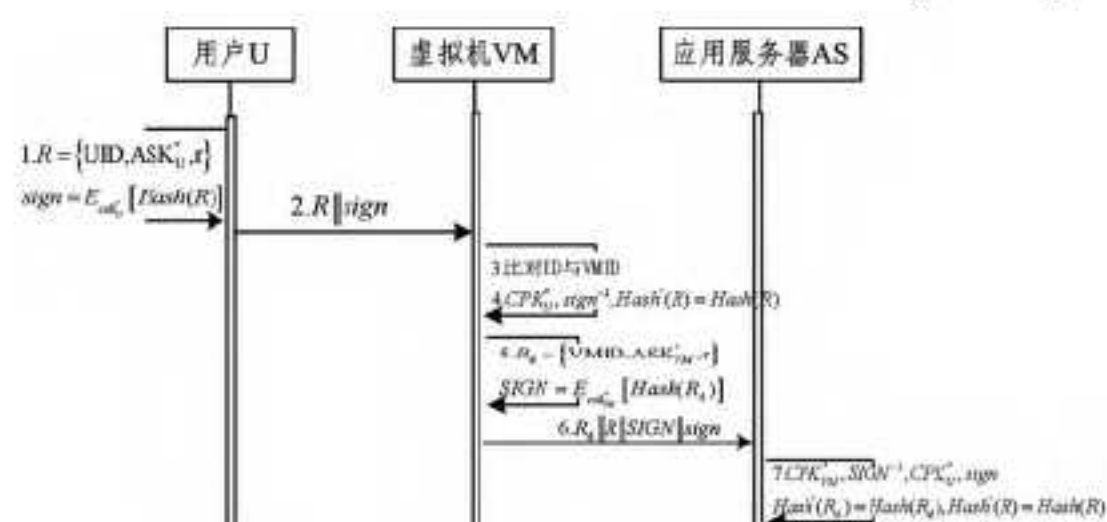


图3 虚拟资源应用认证流程

5 安全与性能分析

在实用性方面,用户与虚拟云桌面服务器、用户与虚拟机、虚拟机与应用服务器之间认证方法均基于CPK 的设计,因此虚拟桌面系统可进行统一管理和维护。CPK 具有密钥产生规模化、动态分发静态管理模式等优点,能够实现超大规模的密钥分发,而且不需第三方在线参与,因此能够满足大量用户认证需求,不会形成性能瓶颈。

在安全性方面,所给出方法将用户标识和虚拟机UIID 绑定成联合标识,可实现用户身份和虚拟机身份的绑定,若与用户认证相结合,则可有效防止虚拟机被攻击后的冒用问题。此外,虚拟云桌面系统中的所有认证均都基于CPK 密码体制,鉴于CPK 自身安全性,系统整体具有较高的安全性。

结束语 本文针对虚拟桌面的特有安全隐患,基于CPK 设计了虚拟资源申请和虚拟资源使用两种场景下的认证方法,并给出了具体认证流程,最后对所提方法进行了安全和性能分析。身份认证是信息安全的基本技术,本文所提认证方法若与身份管理、策略管理相结合,则能够设计出更加有效的虚拟桌面防护方法。此外,CPK 本身特点使得所提方法能够支撑大用户量的认证需求,但由于所提方法为抵御虚拟机被攻击后的冒用问题,将用户与虚拟机进行了绑定,因此该方法适用于用户稳定,且虚拟资源分配较固定的场合。

参考文献

- [1] 郑志勇,吕远大,王毅. 虚拟桌面系统应用安全性分析与对策[J]. 网络安全技术与应用, 2012, 10(10): 50-52
- [2] 孙宇,陈煜欣. 桌面虚拟化及其安全技术研究[J]. 信息安全与通信保密, 2012, 33(6): 87-88, 92
- [3] 宁芝,方正. 涉密信息系统虚拟化安全初探[J]. 保密科学技术, 2012, 22(2): 70-74
- [4] 南湘浩. CPK 密码体制与网际安全[M]. 北京: 国防工业出版社, 2008
- [5] 南湘浩. CPK 组合公钥体制(v8.0)[J]. 信息安全与通信保密, 2013, 34(3): 39-44
- [6] 周加法,马涛,李益发. PKI、CPK、IBC 性能浅析[J]. 信息工程大学学报, 2005, 6(3): 26-31
- [7] 王嘉林. 基于PKI 和CPK 的大规模网络认证方案的对比分析[J]. 保密科学技术, 2012, 6: 44-49
- [8] 汤维. 基于组合公钥密码体制的云安全研究[D]. 武汉: 华中科技大学, 2011
- [9] 马宇驰,赵远,邓依群,等. 基于CPK 的可信平台用户登录认证方案[J]. 计算机工程与应用, 2010, 46(1): 90-94

(上接第369页)

- [20] Paillier P. Public-key cryptosystems based on composite degree residuosity classes[C]// UROCRYPT. 1999: 223-238
- [21] Dean J, Ghemawat S. MapReduce: simplified data processing on large clusters[C]// Proceedings of 6th Conference on Symposium on Operating Systems Design and Implementation (OSDI'04). 2004
- [22] Ishai Y, Kushilevitz E, Ostrovsky R, et al. Batch Codes and Their Applications[C]// Proceedings of the 36th Annual ACM Symposium on Theory of Computing. 2004: 262-271

- [23] Yoshida R, Cui Y, Shigetomi R, et al. The Practicality of the Keyword Search Using Pir[C]// International Symposium on Information Theory and Its Applications (ISITA 2008). 2008: 1-6
- [24] Botelho F C, Galinkin D, Meira W, et al. External perfect hashing for very large key sets[C]// Proceedings of the Sixteenth ACM Conference on Conference on Information and Knowledge Management (CIKM '07). 2007: 653-662
- [25] Botelho F C, Lacerda A, Menezes G V, et al. Minimal perfect hashing: A competitive method for indexing internal memory[J]. Information Sciences, 2011, 181(13): 2608-2625