基于 PKI-USIM 的移动终端安全认证方法

戚 湧,丁玲玲,李千目
(南京理工大学 计算机科学与工程学院,江苏 南京 210094)

摘 要:随着移动通信技术的迅速发展,智能移动终端得到应用普及,大量的第三方应用也随之产生,给移动终端的信息安全带来了很大威胁。为了保护移动终端的信息安全,文中提出一种基于 PKI-USIM 的移动终端安全认证方法。将 PKI 技术与智能卡技术相结合,利用移动终端的 USIM 卡,实现对智能终端第三方应用的安全认证,有效提高移动终端信息的安全。PKI-USIM 对网络环境的适应、运算速度、计算能力、存储容量以及上层应用的扩展开发性能都有很大提高,PKI-USIM 技术对于移动终端用户身份认证的过程具有实用性和安全性,同时也是对智能卡认证应用的一种扩展研究。

关键词:PKI-USIM;身份认证;移动终端;无线网络
中图分类号:TP301 **文献标识码**:A **文章编号**:1673-629X(2015)07-0128-05
doi:10.3969/j.issn.1673-629X.2015.07.028

A Security Authentication Method of Mobile Terminals Based on PKI-USIM

QI Yong, DING Ling-ling, LI Qian-mu
(School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract: With the rapid development of mobile communication technology, intelligent mobile terminals have been applied popularly, it also leads to produce a large number of third-party applications. All of these greatly enrich people's lives, but the information security of the mobile terminals has been threatened. In order to protect the information security of mobile terminals, propose a security authentication method of mobile terminals based on PKI-USIM in this paper. According to the realities of complex wireless network environment, combining the PKI technology and smart card technology, using USIM card of mobile terminals to realize intelligent terminals' authentication, effectively improve the safety of the mobile terminal information. PKI-USIM has adapted to the network environment, its computing speed, computing power, storage capacity as well as the expansion capabilities of upper applications has been greatly improved. PKI-USIM technology is more practical and safer for mobile end-user's authentication process, and it's an extension of research on smart card two-factor authentication applications.

Key words: PKI-USIM; identity authentication; mobile terminals; wireless network

0 引 言

随着移动通信技术和无线网络技术的不断发展,3G/4G 时代的到来,人们对于个人移动通信的要求越来越高。大量的无线移动终端,如智能手机、平板电脑等得到普及应用。在新的无线网络环境中,大量相关的第三方应用也随之产生,极大丰富了人们的生活。然而,在给人们带来便利的同时,也带来了各种安全问题。因此,针对移动终端的信息安全性问题变得日益重要,越来越引起大家的关注。

随着智能手机、PAD 等移动终端功能的日益增强,以及 Android 等开放性操作系统的使用,移动终端正面临着不亚于计算机和互联网的安全挑战。信息泄露、信息破坏、非法访问、窃听假冒、木马病毒等问题,正严重威胁着移动终端的信息安全。针对这些问题,提出了多种安全防护机制和手段,用户身份认证就是其中一种。

在无线网络环境中,用户身份认证是移动终端使用过程中实现信息安全的一项关键措施。对使用频繁、私密性强的移动终端系统而言,确保其的安全,防止非法访问,身份认证有着至关重要的作用。因此,如

收稿日期:2014-08-24 **修回日期**:2014-11-24 **网络出版时间**:2015-06-23
基金项目:国家自然科学基金资助项目(61272419)
作者简介:戚 湧(1970-),男,博士,教授,博士生导师,研究方向为网络信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20150623.1028.018.html

何为无线网络环境中的移动终端建立一套有效的身份认证体系,提高移动终端的安全性能,成为当前研究的关键问题[1-3]。

1　相关技术

1.1　PKI 技术

PKI(Public Key Infrastructure,公钥基础设施)技术以公开密钥技术为基础,为所有的网络应用提供密码服务和相关管理体系,包括加密和数字签名,确保信息的保密性、安全性、完整性以及不可抵赖性。PKI 技术依赖于数字证书的交换,而交换的前提是交换的双方—用户或业务系统,必须事先在 PKI 体系的核心主 CA 系统中进行注册,确保其有合法的身份和权限,用户的信息与真实用户一一对应。利用密码学原理的数字签名,可以保证发送方无法抵赖其所发送的信息内容,接收方也无法伪造信息数据。数字证书中包含用户的数字签名,利用数字签名可以确认当前用户的身份,从而保证信息可以正确、安全地传输。此外,利用数字签名,还能管理本身或者低一级的身份证书。一个完整的 PKI 系统能够完成用户注册、生成密钥、发放证书、恢复密钥、更新密钥、作废证书等功能,能够为用户提供全面的 PKI 服务。因此,典型的完整 PKI 系统应该包括认证结构 CA、证书库、密钥备份及恢复系统、证书作废处理系统、应用接口系统五个组成部分[2-4]。图 1 为 PKI 组成结构示意图。

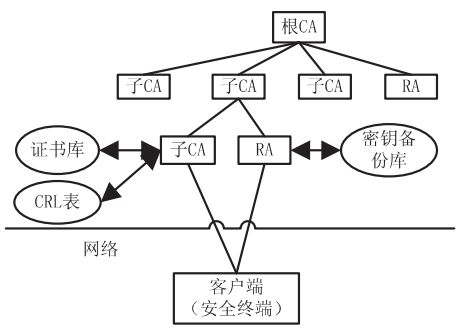

图 1　PKI 组成结构示意图

PKI 技术体系的核心是认证中心(Certificate Authority,CA),体系结构中所有用户都需要向 CA 中心申请注册数字证书,认证中心也会负责签发和管理用户的证书信息,将用户的证书与用户的公钥等其他个人信息进行捆绑操作,方便用户的身份验证。

证书库是数字证书的保存仓库,对公众开放使用。数字证书是由权威第三方机构—CA 认证中心签发的电子文档,符合 X.509 标准,用以验证用户实体的身份。

在 PKI 系统中,为了保证数据的安全性,密钥的存在不可或缺。为了防止密钥丢失,密文无法解密,在 CA 认证中心需要设立密钥的备份与恢复系统。

证书作废处理系统 RA 用以将不再需要的证书清除出证书库,确保数字证书系统的有效使用。

PKI 技术可以应用在众多不同的平台和环境中,利用 PKI 应用接口系统,能够让这些平台更好地与 PKI 进行交互,确保平台数据的安全性、完整性、可靠性、一致性。

在 PKI 体系中,密码学算法是密钥应用管理的关键。PKI 的核心算法是公开密钥算法,即非对称加密算法。在加密和解密的过程中,使用两个不一样的密钥,用公钥进行加密,用对应的私钥进行解密。常见的非对称加密算法有 RSA 算法、安全散列算法以及椭圆曲线加密算法(ECC)等[5-6]。

1.2　智能卡技术

认证的目的是为了让交互的双方确认并且能够建立良好的信任关系,是对数据进行加密的前提。在实际的用户身份认证过程中,可以采用以下三类因素作为认证的基础:①用户的记忆信息,如口令等;②用户的生物特征,如指纹等;③用户的物品,如移动终端的智能卡等。而智能卡具有独立的加密计算和存储能力,不易被逆向工程利用,具有独特的安全优势。智能卡的种类很多,类似于手机 SIM 卡的是微处理器卡,图 2 为微处理器智能卡硬件逻辑关系,包括微处理器 CPU、存储器、I/O 通信单元三个部分,并且通过 I/O 通信单元与卡外部的系统进行通信交互[3]。它独特的硬件、软件等多重保护措施,能够有效地阻止用户对卡内的信息进行非法访问,可以保护卡内的重要信息。另外,利用卡中内嵌的芯片,可以在卡内进行敏感信息的操作,如加密、解密等,不需要读出卡外,从而能够避免卡内信息被外部系统中的木马、病毒程序等感染。因此在身份认证的设计中,常被作为重要的认证因素,成为 PKI 技术较为理想的安全介质[7-9]。

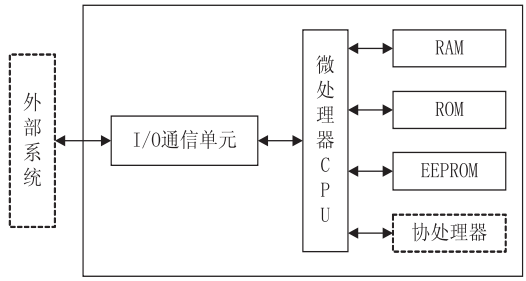

图 2　智能卡硬件逻辑关系

基于 PKI 技术的智能卡有一定的标准,能够提供生成密钥和储存密钥的功能,以及一定的加密解密算法的运算能力。首先,PKI 智能卡具备卡生成、存储密钥对的功能,卡中嵌入 RSA 处理器能够直接实现 RSA 运算,还有部分智能卡中甚至具有 DES 或 SHA-1 等算法的运算能力。如 GPK8000 智能卡就支持 DES 和 RAS 算法。同时,PKI 智能卡还可以解决随机因子的

问题,提供真随机数发生器,提高加密算法的可靠性。使用智能卡储存密钥和证书可以保证私钥完全的隐秘性,只有持有智能卡才能进行相关操作,不用担心私钥被泄露;另外,智能卡随取随用,方便安全携带。

文中提出基于 PKI 技术与智能卡技术相结合的用户身份认证体系,通过将 PKI 技术与移动终端的智能卡相结合,将该技术扩展到第三方应用的身份认证的过程中,实现无线网络环境中对智能终端的信息保护,实现用户的安全接入,从而提高移动终端的信息安全。

2 基于 PKI-USIM 的移动终端安全认证方法

2.1 PKI-USIM

针对移动 3G、4G 等无线网络技术的不断发展,文中将 PKI-SIM 卡技术进行扩展,提出 PKI-USIM 智能卡方案,适应高速发展的网络需求,提供第三方应用的身份认证,力求更好地为移动终端提供安全认证服务。

SIM(Subscriber Identity Module)卡即为“用户识别卡”,采用 A 级加密,用于存储运营商用户的相关数据、鉴权方法,还有密钥信息,可供 GSM 系统,即传统意义上的 2G 网络对用户进行身份认证。此外,SIM 是用户与系统的连接和信息交换的桥梁。而 USIM(Universal Subscriber Identity Module)“全球用户识别卡”实际上属于普通 SIM 卡的升级版,是用户体验 3G/4G 等更高制式网络的前提保障。表 1 为 USIM 卡与 SIM 卡的比较[10]。

表 1 USIM 卡与 SIM 卡在各个方面的比较

	USIM 卡	SIM 卡
应用	基于 UICC(Universal Integrated Circuit Card)平台,同时包括 USIM 和 SIM 两个逻辑模块,可以支持 4 个并发逻辑应用(包括非电信应用,如电子交易等),支持 USIM 卡主动发起的多业务应用,容易进行增值开发	“SIM 模块”是基于卡的操作系统(OS)的开发,功能相对单一,不支持 SIM 卡主动发起的多业务应用,不容易进行增值开发
安全性	USIM 和网络之间的双向鉴权,采用五元组鉴权集,提供安全商务的保证,安全性大大提高	单向鉴权,网络鉴权 SIM,采用三元组鉴权集
电话簿	一个用户可以包含多个电话号码,多个电子邮件地址,多个昵称,存储内容更加丰富	部分 SIM 卡的电话号码簿很简单
机卡接口速率	USIM 卡机卡接口速率大大提高,能够达 230 kbps	大约 57 kbps 左右
STK 功能	USIM 卡支持更丰富的 STK 逻辑通道(除 GPRS 外,还有 UMTS,红外,蓝牙等),使得基于 USIM 卡主动发起多业务成为可能	GPRS

USIM 是移动终端能够在 3G/4G 网络使用的基础,是用户身份安全与应用业务的载体。与普通 SIM 卡相比,USIM 卡不仅能够完成单纯的认证功能,在存储器容量、CPU 处理速度、接口效率等方面都有很大提高。而且,随着科技的进步,USIM 逐渐向移动商务平台、多应用平台发展,为在手机智能卡上开发实现一些上层的应用,如电子钱包、PKI 应用等打下了基础。

PKI 技术与移动终端的 USIM 卡相结合,USIM 卡成为 PKI 私钥和数字证书的最佳载体,也是密码算法的有利提供者。与传统 PKI-SIM 卡相比,PKI-USIM 卡的运算速度、计算能力、存储容量还有应用扩展的水平等都有显著提高,能支持更高的网络制式。面对等级更高、情况更复杂的网络环境,通过 USIM 卡,用户可以更好地完成移动终端的安全认证任务。

2.2 PKI-USIM 安全体系

2.2.1 PKI-USIM 安全认证微操作系统结构

利用 USIM 的硬件、软件特点,通过内核接口、驱动等功能模块,将 PKI 安全体系融入 USIM 芯片的开发,实现卡内部操作系统上层应用的扩展,设计基于 PKI 安全体系的智能卡。文中设计的移动终端身份认证系统使用的 USIM 卡具有随机数发生器和加密协处理器等,然后利用硬件方法,内部实现 RSA 加密算法,针对每一次的传输,在智能卡的芯片内部产生新的密钥对,从而使得在芯片内部就可以完成加密、解密运算。在对用户进行身份认证的过程中,将用户的私钥保存在 USIM 卡的存储器中,通过处理器执行 RSA 算法,完成加解密的任务。PKI-USIM 卡内部微操作系统结构模型如图 3 所示。

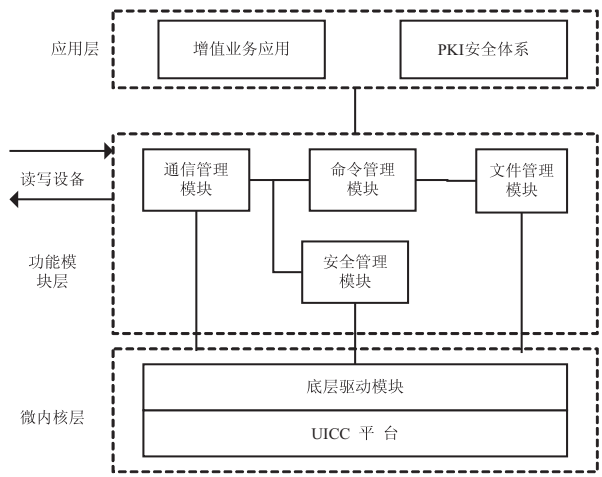

图 3 PKI-USIM 卡内部微操作系统结构模型

2.2.2 PKI 安全认证体系结构

PKI 安全认证体系成为 USIM 卡上安全模块的重要应用,确保用户在使用移动终端过程中完成身份认证过程。USIM 智能卡作为数字储存的介质,保存用户和应用系统所有的数字证书和密钥,通过移动运营商等机构作为认证管理平台,为移动终端的第三方应用进行基于 PKI 技术体系的身份认证、签名和加密解密工作。在对应用进行认证之前,先使用 USIM 卡的 PIN

码验证确保移动终端的合法性[1,11-12]。图 4 为 PKI 安全认证体系的结构图[1,5]。

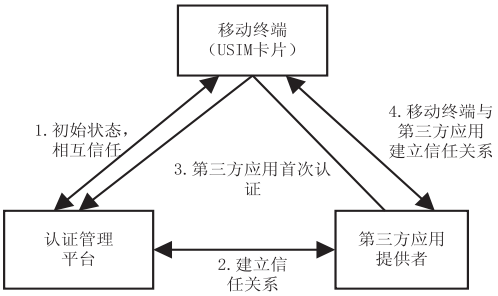

图 4　PKI 安全认证体系的结构

PKI 安全认证体系的管理平台负责接收用户发送的消息和签名信息,从第三方应用提供者查找身份验证的相关信息。当 USIM 卡或第三方应用提供者都为合法用户时,发出证书加载指令,利用自身的私钥对指令消息进行签名,发送给用户。管理平台管理运营商的证书和私钥,以及第三方应用提供者的相关信息。

整个 PKI 安全认证体系中,证书是最重要的构成要素。在用户身份安全认证过程中,证书存放在 USIM 卡的证书库中,在与第三方应用进行通信时,通过相应的设置可以访问卡内的证书库。

利用 PKI 安全认证体系对第三方应用进行身份验证的过程如下:初始时,USIM 智能卡中内置移动运营商的数字证书,移动终端与移动运营商(是认证管理平台的一部分)直接建立相互信任的关系,然后第三方应用提供者与认证管理平台建立信任关系,使应用程序允许 USIM 卡对其进行基于 PKI 安全认证体系的基础服务,当终端与第三方应用提供者首次通信时,应用程序系统需要经过管理平台的验证,如果验证通过,则 USIM 卡可以加载该应用的证书,生成应用的证书和私钥,建立移动终端与应用程序直接的信任关系;最后,当第三方应用提供者与移动终端进行通信时,应用程序提供身份信息给移动终端的 USIM 卡进行身份验证,验证通过后,就可进行加密解密、数字签名等后续操作。

2.2.3　*加密解密、数字签名*

当完成身份认证过程后,返回认证成功的消息,就可以进行数据加密解密、数字签名等操作。在通信过程中,每建立一次连接就生成一个新的会话密钥,保证数据的通信更加安全。整个协商密钥,数据加解密的通信过程如下:

(1)移动终端发起会话请求,生成会话密钥,使用用户的私钥进行签名,然后使用对应服务器端的公钥进行加密,发送给服务器;

(2)接收到加密信息后,服务器端进行解密,使用用户的私钥进行签名验证。若验证成功,则使用服务器端的私钥对公钥进行签名,利用用户的公钥进行加密,发送给移动终端;否则密钥协商失败;

(3)用上述相同的方式进行解密,验证签名;

(4)双方数据的传输都需要利用协商好的会话密钥进行。

基于 PKI-USIM 技术的移动终端安全认证方案,是对传统 PKI-SIM 技术的改进与提高,是对智能卡安全认证应用的扩展,将其利用到第三方应用的身份认证过程当中。希望通过该方案,能够使移动终端的安全性在应用环境愈加复杂的网络中,得到更好保证。

3　认证方法的安全性分析

文中所提方案基于智能卡技术与 PKI 技术,结合所处的复杂的网络环境,提高了移动终端安全认证体系的安全性。

首先,该方案中所有的私钥、数字证书等私密信息都保存在 USIM 卡内部,卡内的信息数据在不匹配的情况下无法被访问。签名运算和加密解密的过程都在卡内实现,对外部的访问不提供接口,因此安全性、私密性可以得到很好的保证。

其次,在 USIM 卡使用的过程中,只有当 USIM 卡与移动终端连接时,才自动将该卡中的所有证书注册到移动终端的证书存储区中,以确保移动终端能够使用用户证书进行身份验证;而当 USIM 卡被拔除后,存储区中的证书信息将会被全部删除。这样的一个存放过程,也确保了用户的信息不出 USIM 卡,不会出现信息泄露的问题,非法用户也无法模拟合法用户完成与移动终端的身份认证。

第三,在完成身份认证之后,对数据进行加密解密,以及数字签名等操作都是在 USIM 卡的片内操作系统的控制下完成的,私钥的释放也是在卡内完成,对卡外的应用程序是不可见的,从而规避了私钥明文的泄露。

第四,提供双因素认证,在对应用进行认证之前,可以先使用 USIM 卡的 PIN 码验证确保移动终端的合法性,防止认证一方的身份假冒,保证数据来源的安全性和不可否性。只有在智能卡丢失和密码泄漏同时发生时,才会破坏系统安全[5-6]。

最后,USIM 卡与 SIM 卡相比,对网络环境的适应、运算速度、计算能力、存储容量还有上层应用的扩展开发性能有较大提高,PKI-USIM 技术对于移动终端用户身份验证的过程更加具有实用性和安全性,同时也是对智能卡双因素认证应用的一种扩展[10]。

4　结束语

针对复杂的无线网络环境,以及移动终端的信息

安全防护,文中将智能 USIM 卡与 PKI 技术相结合,为移动终端提供一种安全可靠的安全认证方案,对众多的第三方移动应用提供身份认证,确保移动终端的信息安全。USIM 卡成为保存私钥、证书的理想载体,在安全存储了个人信息的同时,它的便携性也使它成为开展移动安全业务的理想媒介。

目前,信息技术的发展日益改变着人们传统的工作生活模式。智能手机、平板电脑等移动终端的功能不断加强,终端应用的大量开发使用,移动终端的信息安全正面临着越来越严峻的挑战。随着智能卡等一些安全芯片的处理能力的不断提高,PKI 技术的不断演进,移动终端的安全性一定会得到更大的提高[13]。

参考文献:

[1] Markovié M, Dordevié G. Secure mobile government and mobile banking systems based on android clients[M]//Securing electronic business processes. Fachmedien Wiesbaden: Springer, 2013: 263-273.

[2] 张 杨. 移动终端安全认证的设计与实现[D]. 北京:北京邮电大学,2012.

[3] EI Kettani M D E C, En-Nasry B. MIdM: an open architecture for mobile identity management[J]. Journal of Convergence, 2011, 2(2): 25-32.

[4] Toshikazu N. A distributed authentication mechanism for sharing an overlay network among multiple organizations[C]// Proceedings of the 12th international conference on information integration and web-based applications & services. USA: [s. n.], 2010: 813-817.

[5] 许喆明. 基于 PKI 的智能卡双向身份认证机制的设计与实现[D]. 长沙:国防科学技术大学,2006.

[6] 范亚军. 无线移动网络中的认证密钥交换协议及其应用研究[D]. 北京:北京邮电大学,2012.

[7] 刘百乐. 基于安全 SIM 卡的移动通信研究[J]. 计算机安全,2007(11): 26-29.

[8] Li M, Sandrasegaran K. A proxy based authentication localisation scheme for handover between non trust-associated domains[J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2010(4): 47-50.

[9] Tsai Y R, Chang C J. SIM-based subscriber authentication Mechanism for wireless local area networks[J]. Computer Communications, 2006, 29(10): 1744-1753.

[10] 张李静. 智能卡在移动通信领域的应用:USIM 卡操作系统底层设计、移植与测试[D]. 天津:天津理工大学,2008.

[11] Firoozy-Najafabadi H R, Feizi-Derakhshi M. Multipurpose smart SIM card based on mobile database and location dependent query[C]//Proc of 2012 6th international conference on application of information and communication technologies. [s. l.]: IEEE, 2012: 1-5.

[12] Kuhn D R, Coyne E J, Well T R. Adding attributes to role-based access control[J]. Computer, 2010, 43(6): 79-81.

[13] 滕震方. 基于多属性的移动终端安全接入网络认证协议[J]. 计算机应用与软件,2013,30(8): 43-46.

(上接第 127 页)

veys, 2012, 44(4): 1-41.

[6] Biddle R, Mannan M, van Oorschot P C, et al. User study analysis and usable security of passwords based on digital objects[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 970-979.

[7] 胡 卫,张焕国,魏国珩,等. 面向移动平台的新型身份认证方案设计[J]. 计算机科学,2014,41(4): 99-102.

[8] Chang Tingyi, Tsai Cheng-Jung, Lin Jyun-Hao. A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices[J]. Journal of Systems and Software, 2012, 85(5): 1157-1165.

[9] Cheong Soon-Nyean, Ling Huo-Chong, Teh Pei-Lee. Secure encrypted steganography graphical password scheme for near field communication smartphone access control system[J]. Expert Systems with Applications, 2014, 41(7): 3561-3568.

[10] 黄叶珏,褚一平. 基于多分辨离散模型的图形密码[J]. 计算机工程与设计,2012,33(12): 4493-4496.

[11] Wu Tzong-Sun, Lee Ming-Lun, Lin Hanyu, et al. Shoulder-surfing-proof graphical password authentication scheme[J]. International Journal of Information Security, 2014, 13(3): 245-254.

[12] 潘 源. 防肩窥攻击的图形密码的设计与实现[D]. 北京:北京大学,2013.

[13] 高晶元. 一种防肩窥攻击的图形密码的设计与实现[D]. 北京:北京大学,2008.

[14] Chinasson S, Stobert E, Foret A, et al. Persusive cued click-points: design, implementation and evaluation of a knowledge-based authentication mechanism[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(2): 222-235.

[15] 胡 卫,马常楼,廖 巍. 图形密码方案可用性及安全性分析[J]. 计算机应用与软件,2010,27(12): 55-57.

基于PKI-USIM的移动终端安全认证方法

作者： 戚湧， 丁玲玲， 李千目， QI Yong， DING Ling-ling， LI Qian-mu
作者单位： 南京理工大学 计算机科学与工程学院,江苏 南京,210094
刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2015(7)