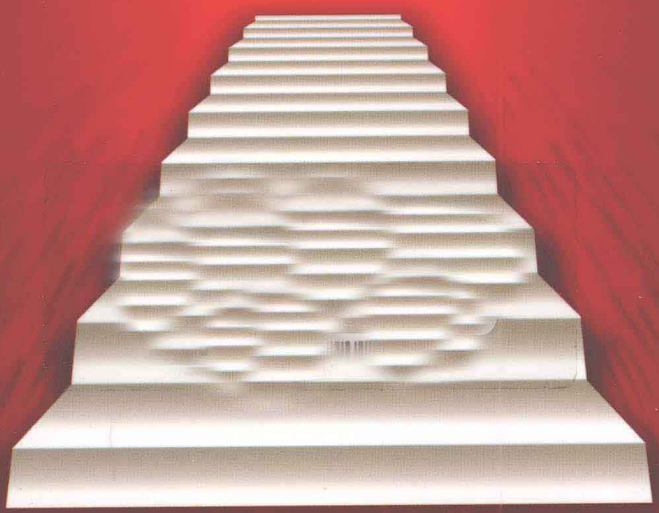
西安交通大学学术文库

信任管理与计算

桂小林　李小勇

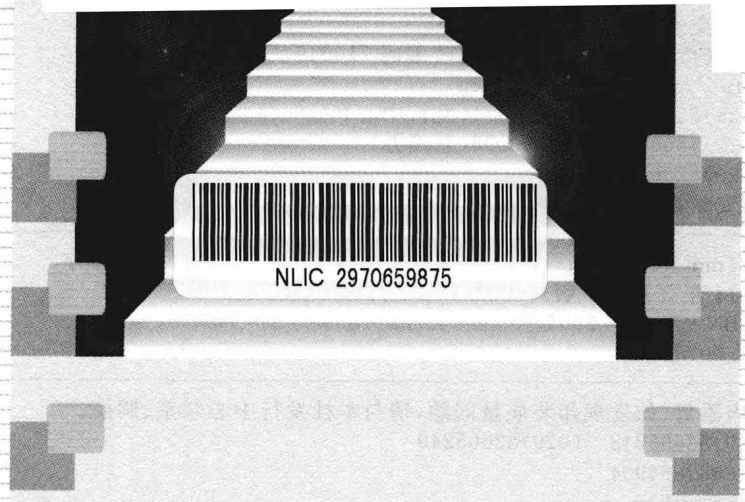


西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

西安交通大学 学术文库

信任管理与计算

桂小林　李小勇



西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

内容简介

信任管理(trust management)技术是解决互联网安全问题的一个重要手段，是实现可信网络与可信计算的重要基石，它对于实现高可信的网络服务环境，支持网络服务大众化、平民化和“所要即得”具有重要的理论意义和现实意义，对于构建高可信的 Peer to Peer(P2P)系统、Content Distribution Network(CDN)系统、web serviers 系统、网格计算系统(grid)和电子商务系统均具有较好的技术参考价值和应用前景。

本书基于国家“863”计划项目和国家自然科学基金项目等方面的研究成果，阐述信任与信任管理的基本概念，基于身份的静态信任管理机制和基于行为的动态信任管理机制，并对上述信任管理机制的应用背景进行了详细论述。

图书在版编目(CIP)数据

信任管理与计算/桂小林，李小勇编著. —西安：西安交通大学出版社，2011.3
ISBN 978-7-5605-3556-2

Ⅰ.①信… Ⅱ.①桂…②李… Ⅲ.①计算机网络-信用-研究 Ⅳ.①TP393

中国版本图书馆 CIP 数据核字(2010)第 083327 号

书　　名　信任管理与计算
编　　著　桂小林　李小勇
责任编辑　李　文

出版发行　西安交通大学出版社
（西安市兴庆南路 10 号　邮政编码 710049）
网　　址　http://www.xjtupress.com
电　　话　(029)82668357　82667874(发行中心)
(029)82668315　82669096(总编办)
传　　真　(029)82668280
印　　刷　西安新视点印务有限责任公司

开　　本　787mm×1092mm　1/16　**印张**　17.875　**字数**　328 千字
版次印次　2011 年 3 月第 1 版　2011 年 3 月第 1 次印刷
书　　号　ISBN 978-7-5605-3556-2/TP·529
定　　价　43.00 元

读者购书、书店添货、如发现印装质量问题，请与本社发行中心联系、调换。
订购热线：(029)82665248　(029)82665249
投稿热线：(029)82664954
读者信箱：jdlgy@yahoo.cn

前　言

随着互联网的快速普及与发展，网络中接入的计算机数量与资源日益增多，通过网络共享各种软、硬件资源，提供统一、开放的计算与信息服务环境，已成为一种趋势。在互联网内，各种资源与环境具有异构性、动态性、分布性和多管理域性等特征，在这样的环境下为用户提供可靠、安全的应用执行环境和信息共享服务，面临着更加严峻的安全技术挑战。

信任管理(trust management)技术是解决互联网安全问题的一个重要手段，是实现可信网络与可信计算的重要基石，它对于实现高可信的网络服务环境，支持网络服务大众化、平民化和"所要即得"具有重要的理论意义和现实意义，对于构建高可信的Peer to Peer(P2P)系统、Content Distribution Network(CDN)系统、web serviers 系统、网格计算系统(Grid)和电子商务系统均具有较好的技术参考价值和应用前景。

信任包括基于身份的信任(identity trust)和基于行为的信任(behavior trust)。基于身份的信任采用静态验证机制来决定是否给一个实体授权，常用的技术包括加密、数据隐藏、数字签名、授权以及访问控制策略等。基于行为的信任通过实体的行为历史记录和当前行为特征来动态判断实体的可信任度，根据信任度大小给出访问权限。

在基于身份的信任管理技术领域，主要提供面向同一组织或管理域的授权认证，从身份可信的角度，通过对软件实体的授权和身份验证确保系统运行的安全性，是可信计算研究的基础问题之一。例如，PKI(Public Key Infrastructure)和 PMI 等技术依赖于全局命名体系和集中可信权威。基于策略和凭证的信任管理系统根据 Blaze 和 Jøsang 等提出的信任管理的概念，在信任网络实体的基础上为用户提供资源访问权限，并以信任查询的方式提供分布式静态信任机制，对于解决单域环境的安全可信问题具有良好效果。

在基于行为的动态信任管理领域，在对信任关系进行建模与管理时，强调综合考察影响软件可信性的多种因素(特别是行为和环境上下文)，针对可信性的多个属性进行有侧重点的建模。强调动态地收集相关的主观因素和客观证据的变化，以一种及时的方式实现对软件实体的可信性评估、管理和决策，并对网络实体的可信性进行动态更新与演化。目前，基于行为的信任管理技术的研究相对滞后，还处于研究的前期阶段，在信任表达、评估、更新、演化和管理等方面还需要进行大量研究工作。

本书阐述了信任与信任管理的基本概念，基于身份的静态信任管理机制和基于行为的动态信任管理机制，并对上述信任管理机制的应用背景进行了详细论述。

全书共分为 10 章：第 1 章论述信任与信任管理技术的概念，阐述信任关系建模方法，介绍可信计算的工作原理和信任管理模型分类等；第 2 章论述基于身份认证的静

态信任管理机制，包括身份认证方法，身份认证的技术基础，PKI 中基于 CA 的信任机制，基于身份的信任模型和基于策略和凭证的信任管理等；第 3 章论述动态信任建模与管理方法，包括动态信任概念模型与总体架构，基于历史证据窗口（HEW）的总体信任度计算模型以及基于动态信任关系的访问控制策略等；第 4 章阐述可信行为监控与感知方法，包括系统行为感知和程序行为感知，程序行为指标定义、获取及量化方法等；第 5 章阐述基于行为序列的动态信任评估方法，包括行为数据的获取与规范化，基于粗糙集和信息熵的直接信任度（DTD）度量和基于 IOWA 算子的 DTD 预测等；第 6 章论述基于机器学习的动态信任评估方法以及相关方法在网络资源自主保护中的应用，包括基于机器学习的动态信任评估模型、算法和资源自主保护机制；第 7 章论述信任推荐与反馈机制，包括基于直接信任树（DTT）的信任反馈计算模型与方法；第 8 章论述信任决策与分配机制，重点阐述权重的自适应分配方法；第 9 章论述信任管理技术在网格环境中的应用技术，包括可行分发、可行调度和基于水印的软件身份鉴别等；第 10 章论述典型应用中的动态信任模型实现方法。

本书由桂小林教授负责组织和统稿，全书内容主要来自如下博士研究生和硕士研究生的研究成果：李小勇（第 3、5、7、8 章）、赵娟（第 4 章）、徐显椋（第 9 章）、陈菲菲（第 6 章）等，在此深表感谢。

本书深入浅出，可作为博士研究生和硕士研究生阶段的“可信计算”、“信任管理”和“信任计算”等课程的教材使用，也可作为大学高年级网络与信息安全课程的辅助教材，同时也是研究生和高校教师从事“网络安全”、“可信网络”、“可信软件”、“信任管理”等方向研究的教学或科研参考书。

本书的研究工作受到国家“863”计划项目（2008AA01Z410）、国家自然科学基金项目（60873071）、教育部“新世纪优秀人才计划”项目（NCET-05-0829）和教育部“网络工程”第二类特色专业建设点（TS-2387）项目等的支持，特此致谢。

本书在撰稿过程中，由于时间急迫，书中错误在所难免，希望读者热情指出，作者将不胜感谢。

作者

2009 年 12 月

于西安交通大学

目　录

第 1 章　信任与信任管理概述

信任(Trust)是构建现实社会和谐关系的基础，也是构建网络社会和谐关系的基石。在计算机网络系统中，包括各种相互关联的实体，如用户、计算机、网络、存储等，这些实体间相互作用，关系日益复杂，如何构建这些实体间的信任关系成为非常复杂的研究课题，也是推动计算机网络应用快速发展的原动力。本章主要围绕计算机科学中的信任的概念、传统的可信计算技术，信任模型、信任管理技术等方面的内容展开介绍。

1.1　信任

信任的研究历史非常悠久，是一种跨学科性的交叉研究，早期的信任理论研究主要涉及到心理学、社会学、政治学、经济学、人类学、历史及社会生物学等多个领域。随着时代的发展，它又融入了商业管理、经济理论、工程学、计算机科学等应用领域知识。

长期以来，信任被认为是一种依赖关系。值得信任的个人或团体意味着他们寻求实践政策，道德守则，法律和其先前的承诺，信任是人类社会一切活动的基石。

1.1.1　信任的定义

从社会学的角度看，“信任”一词解释为“相信而敢于托付”。信任是一种有生命的感觉，也是一种高尚的情感，更是一种连接人与人之间的纽带。《出师表》里有这样的一句话：“亲贤臣，远小人，此先汉所以兴隆也；亲小人，远贤臣，此后汉所以倾颓也。”诸葛亮从两种截然相反的结果中为我们提供了信任对象的品格。可见信任是架设在人心的桥梁，是沟通人心的纽带，是震荡感情之波的琴弦。

“信任”这一概念曾在诸如心理学、社会学、政治学、经济学、人类学、历史及社会生物学等多种不同类型的社会学文献中提及与应用，学者们也曾试图从各个角度出发对信任予以界定(见表 1 - 1)。从这些文献可以看出：信任与可预测、可靠性、行为一致性、能力、义务、责任感、动机、可以耐性、专业技能、可信任性、行为预期等概念密切相关。

表 1-1 中列举了信任的几个经典观点与认识，其中 Rindeback 和 Bantel 的观点把信任看成是存在于个人内部的性格特质或信念。而 Bantel 只是提到了对他人言行方面的信任，Rindeback 则更进一层，涉及对他人的动机、人格方面的信任。Hartman 的理解反映了 Deutsch 认为的信任具有一定程度的冒险性这一点，信任是一个两人共有概念的看法。Deutsch 针对人际信任所下的定义把信任行为等同于合作行为，进而从行为层面来定义信任，为信任的实证研究提供了一条有益的途经。通过多年的探究，人们已经认识到信任是人类社会的重要基石之一，在社会科学、技术科学、商业等诸多领域中，尤其在人们的日常生活中，信任都时刻发挥着决定性的作用。

表 1-1 对信任的几个经典认识

作者	观点
Rindeback[1]	信任是个体对他人言辞、承诺以及口头或者书面陈述可靠性的一种概括化的期望。
Bantel[2]	信任是个体所具有的、构成其一部分个人特质的信念，这种信任认为一般人都是有诚意并且信任别人的。
Hartman[3]	信任是交往双方共同持有的，对于两人都不会利用对方脆弱性(Vunerability)的信心。
Deutsch[4]	信任可由选择相信他人的合作行为来显示。

可见，信任的确是一个相当复杂的社会“认知”现象，牵扯到很多层面和维度，很难定量表示和预测。每个人对“信任”的理解并不完全相同，下面是韦氏和牛津两个著名词典中对信任(Trust)的解释。

①韦氏词典：Firm reliance on the integrity, ability, or character of a person or thing(对某人或某事的正直、能力或性格的坚定依靠)。

②牛津词典：The firm belief in the reliability or truth or strength of an entity (对一个主体的可靠性或真实性或实力的坚定信心)。

上述词典中，简单抽象地描述出了信任的内涵。但是在计算机科学中，这一描述显得不够确切。一般意义上讲，大多数学者对信任的理解可以归纳为：“对实体在某方面行为的依赖性、安全性、可靠性等能力的坚定依靠。”我们将这一理解规范化，再参考 ITUT 推荐标准 X.509 规范[5]，则信任的定义可以表述为：当实体 A 假定实体 B 严格地按 A 所期望的那样行动，则 A 信任 B (Entity A trusts entity B when A assumes that B will behave exactly as A expects)。从这个定义可以看出，信任涉及假设、期望和行为，这意味着信任是很难定量测量的，信任是与风险相

联系的，并且信任关系的建立不可能总是全自动的。

1994 年，Marsh [6]在其博士论文中针对多代理系统中的信任与协作问题，系统地阐述了多代理系统中信任的形式化问题，为信任在计算机领域尤其是互联网中的应用奠定了基础。1996 年，Blaze[7]为解决 Internet 上网络服务的安全问题，提出了“信任管理(trust management)”的概念，并首次将信任管理机制引入到分布式系统之中。

随着以互联网为基础的各种大规模开放应用系统(如网格、普适计算、云技术、P2P 计算、Ad hoc 网络和 Web 服务等)的相继出现和应用，信任关系、信任模型和信任管理的研究逐渐成为信息安全领域中的研究热点。

然而，到目前为止，对于计算机领域中的信任，学术界仍然没有一个准确和统一的定义，不同的文献对信任的理解各不相同，提出了各种不同的定义，据 Welty 等人统计[8]，到 2001 年为止，对“信任”的各种不同的定义就达到 65 种之多。1999 年，Jøsang 等人首先从主观逻辑着手对信任进行量化研究[9]。Grandison 和 Sloman 对各种形式的信任定义进行了综合分析[10]，对这些定义做了比较研究之后，给出的“信任”定义为：“一种坚定的信念，针对的是某个实体能够在某种给定的上下文环境下可靠、安全、可依赖地采取行动的能力。”他们认为信任是一个由很多不同属性组成的概念，包括可靠性、可依赖性、诚实性、真实性、安全性、实力性和及时性，需要根据信任所处的具体环境进行相应的考虑和定义。

而 Dimitrakos[11]从另一个角度对“信任”给出了定义：“A 方对 B 方相关于服务 X 的信任指的是 A 方对 B 方的一种可以预测的信念，针对的是 B 方能够在给定时段给定上下文环境下与 X 相关的活动中可依赖地加以表现。”在这个定义中，某“方”可以是一个单独的实体，一组人或者进程，或者一个系统；术语“服务”的范畴很广，包括事务、推荐、发行证书等；“可依赖性”泛指安全性、保险性、可靠性、及时性和可维性；某个时段可以是服务的一段服务时间或者整个时段，而术语“上下文环境”指的是相关的服务协议、服务历史、技术架构以及可能采用的立法约束框架等。

综上所述，虽然在不同的学科领域，对信任的理解也不尽相同，但是，基本的共识有以下几点：

①信任表征着一个实体的诚实、真实、能力以及可依赖程度；

②信任建立在对实体历史行为认知的基础上；

③信任会随着时间延续而导致对实体认知程度下降而衰减；

④信任是实体间相互作用的依据。

显然，信任会在一定范围内随着实体间多次的接触而动态变化。信任关系的建立除了通过直接认知，获取知识进行决策这一途径外，还可以通过间接途径，获取间接知识(如推荐)来参与决策。

根据上面的分析，本书对信任定义如下："信任表征对实体身份的确认和其本身行为的期望，一方面是对实体的历史行为的直接认知，一方面是其他实体对该实体的推荐。信任可以随实体行为动态变化且随时间延续而衰减。"

1.1.2 信任的分类

信任可以分为基于身份的信任(identity trust)和基于行为的信任(behavior trust)两部分。后者进一步可以分为直接信任(direct trust)和间接信任(indirect trust)。间接信任又可称为推荐或者声誉(reputation)。

1. 基于身份的信任

基于身份的信任采用静态验证机制(static authentication mechanism)来决定是否给一个实体授权。常用的技术包括认证(authentication)、授权(authorization)、加密(encryption)、数据隐藏(data hiding)、数字签名(digital signatures)、公钥证书(public key certificate)以及访问控制(access control)策略等。

当两个实体 A 与 B 进行交互时，首先需要对对方的身份进行验证。这也就是说，信任的首要前提是对对方身份的确认，否则与虚假、恶意的实体进行交互，很有可能导致损失。基于身份的信任是信任研究与实现的基础。在传统安全领域，身份信任问题已经得到相对广泛的研究和应用。

认证(authentication)是实现基于身份信任的访问控制的前提和基础，它是系统核查用户身份的一个过程，保证某个用户或者某个事务的真实性。用户名加口令的方式，就是最为常见的一种认证方式。系统将访问者提供的用户名和口令跟系统保存的数据进行核对，判断用户是否真实可信，这就是一个认证的过程。用户名加口令的方式，虽然安全性较差(因为用户名和密码可能被盗，或者被暴力破解，在网络上这种情况经常发生)，但是由于其实施简单，容易理解，仍然被广泛使用。现在较为安全的认证方式，一般都采用非对称加密协议和算法来完成，也就是一般所说的 PKI 认证。

认证技术分为身份认证和信息认证两个方面，前者用于鉴别用户的身份，后者用于保证通讯双方的信息完整性和不可抵赖性。在达到基本的安全目标方面，两种类型的认证都具有重要的作用。认证是访问控制业务的一种必要支持，访问控制的执行依赖于认证。

授权(authorization)是安全策略配置的基本组成部分。所谓授权，是指赋予主体(用户、终端、程序等)对客体(数据、程序等)的支配权利，规定了谁可以对什么做些什么(Who can do what to what)。

加密(encryption)算法有对称和非对称两种方法。加密和解密使用同一个密钥称为对称密钥，不同则为非对称密钥。公钥系统使用的是非对称密钥，即一个私有密钥和一个公开密钥。加密算法的最好的例子是 RSA(Rivest, Shamir and

Adleman)和 DES(Data Encryption Standard)。公开密钥算法使用的密钥具有唯一的对应性,即一个私钥只对应一个公钥,反之亦然,公钥对外公开,私钥个人秘密保存。一般的使用方法是,发送方用自己的私钥进行签名,然后用接受方公钥来加密,接受方接到信息以后,先用自己的私钥进行消息解密,再用发送者公钥进行签名验证。算法的加密强度主要取决于选定的密钥长度。和对称密钥算法相比,公开密钥算法最大的优点是私钥不需要在网上传递,不会有被攻击者截取的可能。

数字签名(digital signature)是使用公钥体系来防抵赖的一种技术。对一个数字对象进行签名的过程就是签名者计算该对象和他自己的私钥的哈希函数值,利用签名者公钥可以对签名进行认证,然后确定消息发送者的身份。一个合法的签名可以保证签名者的真实性,签名具有不可修改性。

公钥证书(public key certificate)就是网络通讯中标志通讯各方身份信息的一系列数据,它提供了一种在 Internet 上验证身份的方式,其作用类似于日常生活中的身份证,是由公钥证书的发行者为用户发布的关于公钥的描述。公钥证书由发行者加密签名,任何人都可以验证它的完整性,但不能对其进行修改。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。一般情况下证书还包括密钥的有效时间,发证机关(证书授权中心)的名称以及该证书的序列号等信息。目前的国际标准 X.509 数字证书包含以下内容:版本信息、序列号、签名算法、发行机构、有效期、所有及其公开密钥、发行者对证书的签名等。

当一个证书有效日期超期或者证书所包含的信息不再合法时,应该对其撤销,声明该证书的信息不再有效。证书撤销可能是因为用于签署该证书的私钥丢失(此时由该私钥签署的所有证书都应该撤回),也可能是因为包含在证书中的信息已经不再准确。

公钥基础设施 PKI(Public Key Infrastructure)是一个用公钥概念与技术来实施和提供安全服务的具有普适性的安全基础设施。作为一种遵循标准的密钥管理平台,PKI 提供会话保密、认证、完整性、访问控制、源不可否认性、目的地不可否认性、安全通信、密钥恢复等安全服务。PKI 采用公钥证书进行密钥管理,通过第三方认证机构 CA 绑定用户信息及其公钥来验证通信双方的身份,保障信息安全。第三方认证机构 CA 是整个公钥基础设施的关键部分。

PKI 作为一项基础设施,可以解决绝大多数的网络安全问题,经过多年的发展,它已经成为一套成熟的理论,并且初步形成了一套完整的解决方案。然而,由于 PKI 系统在建设的成本及使用的复杂性,使得它在实际的应用中面临着诸如证书管理、验证、撤销等许多复杂的问题,尤其是在不同的 PKI 之间需要交叉认证的时候。为了弥补当前 PKI 存在的不足,降低部署的成本和使用的难度,科学家提出了多种解决方案,如基于身份加密(Identity-Based Encryption,IBE)的方案等。IBE 方案可以用任意的关于用户身份的字符串作为该用户的公钥,用户可以向可

信第三方证明自己的身份并获得私钥。相比 PKI，IBE 最大的优势就是不需要对证书进行管理，因此实现起来非常简单、高效，它为解决网络安全问题提供了一种新的有效方法。

2. 基于行为的信任

随着 Internet 技术的快速发展，网络中接入的计算机数量与资源日益增多，出现了许多新兴的、大规模的分布式应用系统与技术，比如 P2P、网格和云服务。这些技术聚合网络上各种软、硬件资源，提供统一、开放的计算与信息服务环境。在如此开放、异构、动态、分布的网络应用环境中，为用户提供可靠、安全的应用执行环境和信息共享服务，面临着更加严峻的安全技术挑战。尽管采用基于身份的信任机制能够一定程度地保护网络应用系统的安全，但明显存在以下问题。

首先，在基于身份信任的系统中，必须事先确定管理域内、管理域间的资源是可信赖的、用户是可靠的、应用程序是无恶意的。但在这样的大规模网络应用系统中，交互实体间的生疏性以及共享资源的敏感性成为跨管理域间信任建立的屏障。由于网络涉及数以百计的、处在不同安全域的计算资源，显然大量的计算资源的介入将导致无法直接在各个实体（如应用、用户与资源）间建立事先的信任关系。

其次，在基于身份信任的系统中，随着时间的推移，原先信赖的用户或资源也可能变得不可信，期望所有的用户对他们的行为负责是不现实的。因为许可应用程序在计算资源上运行，这时网络资源会被应用程序部分的控制，恶意用户可以通过运行应用程序来攻击系统。在这种情况下，一个合法注册用户如果是恶意用户的话，其完全可以通过在网络应用环境上执行应用程序（或任务）来发现计算机系统的漏洞、获取其他用户的信息资源，甚至攻击系统，破坏网络资源的完整性。

为了解决上述问题，引入了基于行为的信任机制。基于行为的信任通过实体的行为历史记录和当前行为特征来动态判断实体的可信任度，根据信任度大小给出访问权限。基于行为的信任针对两个或者多个实体之间交互时，某一实体对其他实体在交互中的历史行为所做出的评价，也是对实体所生成的能力可靠性的确认。采用行为信任，在实体安全性验证的时候，往往比一个身份或者是授权更具有不可抵赖性和权威性，也更加贴合社会实践中的信任模式，因而更加贴近现实生活。

1.1.3 信任的属性

1. 信任的主观性

信任是授信方（主体）对受信方（客体）的一种主观判断，不同的实体具有不同的判定标准。即便对于同一客体在相同的上下文环境、相同时段、相同行为，根据主体方的不同，给出的可信性判断也很有可能不同。