高等学校信息安全系列教材

计算机系统与网络安全技术

周世杰　陈伟　罗绪成　编著

高等教育出版社
HIGHER EDUCATION PRESS

高等学校信息安全系列教材

计算机系统与网络安全技术

Jisuanji Xitong yu Wangluo Anquan Jishu

周世杰　陈　伟　罗绪成　编著

高等教育出版社·北京
HIGHER EDUCATION PRESS　BEIJING

内容提要

本书是在作者多年从事信息安全研究和教学的工作基础之上，结合计算机系统与网络安全的最新发展动态编写而成的，力求全面涵盖计算机系统与网络安全的各种防御技术。全书共分为9章，内容包括信息安全概述、TCP/IP协议族及其面临的安全威胁、网络安全隔离技术、网络安全技术、协议安全技术、计算机系统物理安全技术、计算机系统可靠性技术、操作系统安全技术、安全审计与计算机取证技术等。

本书内容全面，不仅涵盖计算机系统与网络安全的基础知识，也包括作者在信息安全领域的最新研究成果及技术发展趋势。

本书适合作为高等学校信息安全、计算机、信息对抗以及相关专业高年级本科生以及低年级研究生的教材，也可作为信息安全及相关领域工程技术人员的参考书。

图书在版编目(CIP)数据

计算机系统与网络安全技术/周世杰，陈伟，罗绪成编著．—北京：高等教育出版社，2011.8

ISBN 978-7-04-032458-7

Ⅰ.①计… Ⅱ.①周… ②陈… ③罗… Ⅲ.①计算机系统-高等学校-教材②计算机网络-安全技术-高等学校-教材 Ⅳ.①TP3

中国版本图书馆CIP数据核字(2011)第139602号

策划编辑 武林晓	责任编辑 李善亮	封面设计 于文燕	版式设计 王 莹
插图绘制 尹 莉	责任校对 俞声佳	责任印制 田 甜	

出版发行	高等教育出版社	咨询电话	400-810-0598
社 址	北京市西城区德外大街4号	网 址	http://www.hep.edu.cn
邮政编码	100120		http://www.hep.com.cn
印 刷	廊坊市科通印业有限公司	网上订购	http://www.landraco.com
开 本	787mm×1092mm 1/16		http://www.landraco.com.cn
印 张	18	版 次	2011年8月第1版
字 数	400千字	印 次	2011年8月第1次印刷
购书热线	010-58581118	定 价	27.00元

物料号 32458-00

前　言

计算机系统与网络安全是一个非常复杂的系统工程，其内容包括计算机系统与网络基础理论与技术、网络安全基础理论与技术、协议安全理论以及主机安全技术等。本书从一个全新的角度对计算机系统与网络安全技术进行全面介绍，内容不仅包括常见的防火墙技术、入侵检测技术、容灾技术、协议安全技术，也包括系统物理安全、可靠性、审计以及计算机取证技术等。此外，本书结合 Windows 和 UNIX 操作系统对有关操作系统的防御理论及技术进行系统性介绍。

本书是在作者多年从事信息安全研究和教学的工作基础之上编写而成的，力求全面涵盖计算机系统与网络安全的各种防御技术，以及作者在信息安全领域的最新研究成果。全书共分为 9 章，内容包括信息安全概述、TCP/IP 协议族及其面临的安全威胁、网络安全隔离技术、网络安全技术、协议安全技术、计算机系统物理安全技术、计算机系统可靠性技术、操作系统安全技术、安全审计与计算机取证等。

第 1 章为信息安全概论。本章将对信息、信息技术与信息安全技术的基本概念和内涵进行简单分析，重点介绍安全服务、安全机制及其相互关系，结合网络协议的分层，介绍安全服务的部署与实现。另外，本章从不同的角度介绍了关于信息安全的基本概念。

第 2 章为 TCP/IP 协议族及其面临的安全威胁。本章以计算机网络的分层结构为出发点，分别介绍了 OSI 七层架构和实际使用的 TCP/IP 架构。然后，针对 TCP/IP 的各层分别进行说明，介绍了其中的重要协议以及与协议相关的安全威胁和对策。

第 3 章为网络安全隔离技术。本章主要介绍网络隔离的基本概念、常用的网络隔离设备及隔离方法。网络地址转换与网络隔离有密切联系，因此本章还对网络地址转换的相关内容进行了介绍。物理隔离是网络隔离的主要内容，因此是本章的重点。

第 4 章为网络安全技术。本章首先介绍主流的网络安全模型，包括 PDR 模型、PPDR 模型、PDRR 模型、APPDRR 模型和 PADIMEE 模型。然后以网络安全模型为指引分别从安全预警、安全保护、安全检测以及安全响应等方面介绍了主要的网络安全技术。

第 5 章为协议安全技术。本章的重点是安全协议攻击及其防御方法。Kerberos 协议是基于对称加密算法的双向认证协议，而 X.509 是基于公钥算法的认证协议，这两个协议是认证协议的典型代表。电子商务对安全需求具有特殊性，SET 和 SSL 协议是目前该领域应用最广泛的协议。

第 6 章为计算机系统物理安全技术。本章的重点是计算机系统物理安全及其主要内容。机房安全及电磁辐射保护是环境安全的重点，设备防盗、防毁是设备物理安全的关键，而灾难保护是系统物理安全的关键。

第 7 章为计算机系统可靠性技术。本章对计算机系统的可靠性原理、相应的可靠性保障技

术,以及计算机系统的容错技术和容灾技术进行较详细的说明。

第8章为操作系统安全技术。本章主要从操作系统安全基础、身份认证和访问控制3个方面讨论系统安全的相关问题。同时,对UNIX系统和Windows系统典型的安全问题进行分析,讲解操作系统实现安全保护机制的方法。

第9章为安全审计与计算机取证技术。本章介绍安全审计和计算机取证技术。安全审计和计算机取证技术是其他信息安全防御技术的有力补充,是震慑和打击计算机犯罪的重要手段。

周世杰负责第1章、第3章、第5章以及其他部分章节的编写工作,并负责统稿工作。陈伟负责第4章、第7章、第9章以及其他部分章节的编写工作。罗绪成负责第2章、第6章、第8章以及其他部分章节的编写工作。赵洋参与了第5章部分内容的编写工作。在本书完稿之际,作者要衷心感谢所有对本书出版作出贡献的人,特别是电子科技大学信息安全系的所有教师,他们为本书的顺利出版做了大量有益的工作。还要感谢中国矿业大学的曹天杰对本书的审阅,是大家的共同努力才使得本书得以面世。

由于时间仓促和水平所限,内容难免有所疏漏,恳请读者批评指正,使本书得以进一步改进和完善。作者联系方式:sjzhou@uestc.edu.cn。

编 者

2011年4月

目　录

第 1 章　信息安全概述

随着通信技术、计算机技术和自动控制技术的发展，特别是通信技术和计算机技术的结合，使互联网(Internet)成为人们日常工作、生活不可缺少的一部分。与此同时，信息安全问题也日渐突出，并成为计算机及网络技术普及与应用的主要障碍之一。为此，掌握信息安全基础理论知识，把握信息安全技术发展动态，了解安全威胁及其预防方法，不仅具有重要的现实意义，也具有重要的社会意义和政治意义。

本章主要介绍信息与信息安全的基本知识，并重点介绍信息安全体系的有关内容。

1.1　信息及信息安全

1.1.1　信息

信息(information)的定义有很多，其中较为通用的定义来自于信息论的创始人香农(C. E. Shannon)。香农认为，信息是对事物不确定性的度量，并进而采用信息量来描述信息。本质上，信息反映了事物的形式，描述了不同事物之间的关系和差异。为了更好地理解信息的内涵，可以从信息的来源和信息的性质进行分析。

从信息的来源来看，信息是事物运动的状态和状态的变化方式，因此信息来源于物质。但是，由于信息可寄生于各种媒体之中(例如 Internet)，因此信息也可独立于物质而存在。信息也可来源于人类的精神世界，因为人类的思维活动也属于事物的运动之一。

从信息的性质来看，它具有客观性、普遍性、相对性。客观性是指信息总是具体的，可以被人类所感测、传递、认知、再生和控制。普遍性是指在信息社会中，信息已经如同电力、交通等基础设施一样，成为人们生活中不可缺少的组成部分。相对性是指不同的观察者从同一个事物可以获得不同的信息，比如建筑师看一栋大厦可能被其建筑风格所吸引，而普通用户则更关心其内部结构。

1.1.2　信息技术

联合国教科文组织对信息技术(information technology)的定义是：应用在信息加工和处理中

的科学、技术与工程的训练方法与管理技巧;上述方法和技巧的应用;计算机及其人、机的相互作用;与之相应的社会、经济和文化等各种事物。简而言之,凡是能扩展人的信息功能的技术,都是信息技术。因此信息技术不仅指与计算机相关的技术,凡是用科学的方法解决信息处理和加工中的问题的一切技术(包括实际的应用和理论上的方法、技巧等),都属于信息技术。虽然信息技术不仅仅与计算机技术相关,但是计算机的诞生极大地促进了信息技术的发展。此外,通信技术和网络技术对现代信息技术也有重要影响。

从对信息的处理过程来看,信息技术也指在计算机和通信技术的支持下,对信息进行获取、传递、存储、处理、使用、分配和控制的方法和技术的总称。信息获取是信息的感知与识别问题,其作用是扩展人获取信息的感官功能。它包括信息识别、信息提取、信息检测等技术(这类技术的总称是"传感技术")。信息的传递是指信息在不同信息载体之间的转移。各种通信技术都属于信息传递这个范畴。由于存储、记录可以看成是从"现在"向"未来"或从"过去"向"现在"传递信息的一种活动,因而也可将它看成是信息传递技术的一种。信息处理包括对信息的编码、压缩、加密等。在对信息进行处理的基础上,还可形成一些新的更深层次的决策信息,这称为信息的"再生"。信息使用是信息过程的最后环节,其中涉及控制技术、显示技术等。由上可见,传感技术、通信技术、计算机技术和控制技术是信息技术的四大基本技术,其中现代计算机技术和通信技术是信息技术的两大支柱,它与生物技术、航天技术、新能源技术、新材料技术等被视为20世纪的重大科技成果。

1.1.3 信息安全

安全与不安全(即危险)是相对的,因此远离危险状态即可称之为安全。司机闯红灯是一种危险。相反,如果遵守交通法规而等待,就是远离危险状态,可以认为是安全的。至于什么是危险,不同的人可以有不同的理解。道路中间有一个积水的大水坑,对小孩子来说可能是危险的,而对于一个健康的成人来说则算不上危险。同样,对没有自制能力的学生来说,玩网络游戏可能是危险的,而对于有很强自制能力的学生来说,可能也算不上危险,因此是安全的。总之,从危险的对立面来理解安全,虽然有助于理解安全的含义,但是容易带来认识和理解上的分歧。为此,必须结合具体的情况来分析安全的确切含义。

结合对安全的认识,可以认为使信息远离危险状态即为信息安全。但是,如同上面对安全的分析,这种看法也易导致对信息安全在认识和理解上产生分歧。通常的做法是,根据信息安全所具备的基本性质来分析信息安全的含义。

人们对信息安全的认识和理解也有一个历史过程。在20世纪60年代,一般的观点是信息安全就是通信安全,因此信息安全的主要内涵,是研究如何对信息进行编码后在通信信道上传输,从而防止攻击者通过窃听通信信道来获取信息。

进入20世纪80年代,研究人员开始采用信息安全及其属性来描述其内涵。为此,机密性、完整性和可用性等基本属性成为信息安全的主要内容。美国国家信息基础设施(National Information

Infrastructure,NII)计划认为,信息安全的基本性质包括完整性、可用性、保密性、可靠性和不可抵赖性。数据完整性(integrity)表明数据没有遭受以非授权方式所作的篡改或破坏。可用性(availability)是指经过授权的实体在需要时可请求访问资源或服务。所谓实体,就是指信息系统的参与者(例如人、进程、线程、设备等)。机密性(confidentiality)也称为保密性,是指信息不泄露给非授权的实体,不为其所用。可靠性(reliability)是指系统在规定的条件下和规定的时间内完成指定功能的概率。不可否认性(non - repudiation)也称为不可抵赖性,是指保证消息的发送者和接收者无法否认自己所进行的操作或行为等。此外,从保证国家利益的角度来看,可控性也是信息安全的基本属性。可控性(controllability)是指对信息传播(即内容)具有控制能力的特性。

信息安全的基本目的就是使得上述安全的基本属性得以保证。因此,信息安全是指为了保证信息的基本属性(如完整性、可用性、保密性、可靠性、不可抵赖性和可控性等)所需的全面的管理、规程和控制。其中,管理强调必须对信息施加人为的控制;规程强调从标准和法规等角度来规范实现信息安全的过程和行为;控制则强调必须有相应的工具或服务来保证信息安全得以实现。

另外一种理解信息安全的观点是采用"信息保障"(Information Assurance,IA)的概念。在信息保障框架下,从信息保护过程的角度提出了信息安全应包括以下内容:保护(protect)、检测(detect)、反应(react)和恢复(restore)。保护是指利用数据加密、用户认证、访问控制等技术保证数据的各种属性(如机密性、完整性、可用性等)。检测是指利用各种技术手段,检测并记录危及信息安全的各种攻击行为,并提供事后审计和查询功能。反应是指在检测出攻击行为之后,在攻击过程中或者攻击结束后采取必要的策略,避免攻击再次发生,或者减少攻击行为带来的破坏。恢复是指在攻击对信息或信息系统已经造成破坏后,采用数据恢复、应用恢复等方式,尽量使信息或信息系统恢复到被破坏前的状态。在信息保障框架下,保护、检测、反应和恢复是一个统一的过程。

1.2 信息安全体系

信息安全服务和安全机制均是信息安全体系结构(security architecture)的主要内容。所谓信息安全体系结构,是指对信息和信息系统安全功能的抽象描述,它从整体上定义了信息及信息系统所提供的安全服务、安全机制以及各种安全组件之间的关系和交互。例如,信息安全体系结构决定了用于防御攻击的方法、方案或系统(包括软件和硬件)以及它们之间的相互关系和信息交互活动。安全体系结构主要包括安全策略、风险分析、安全服务、安全机制和安全管理等内容。其中,风险分析是前提,安全策略是核心,而安全机制和安全服务是基础。

风险分析是用于分析信息系统的威胁和脆弱性以及资源或系统功能失效所带来的影响的过程。例如,可以采用列出威胁及脆弱性、列出可能的控制和防御方法和措施、进行成本与效益分析等方法,来对信息或信息系统所面临的风险进行分析。风险分析的结果是采取有效防御措施

(如制定安全计划)的主要依据之一。

安全策略(security policy)是适用于安全域的一组规则。所谓安全域(security zone),是属于一个组织的资源集合。因此,安全策略规定了对各种资源的访问权限:什么是允许的,什么是不允许的。定义安全策略常用的方法有两种:其一是凡是没有被具体规定的,就是允许的;其二是凡是没有被具体规定的,就是不允许的。从内容来看,安全策略包括制度、技术、管理。其中,管理是安全策略中极为重要的内容。信息安全领域有"三分技术,七分管理"的观点。

安全服务、安全机制及其关系也是信息安全体系结构中的重要内容。ISO 7498 从体系结构的角度,描述了 ISO 参考模型中必须提供的安全服务及安全机制,并说明了安全服务及其相应机制在安全体系结构中的关系,从而建立了开放互连系统的安全体系结构框架。下面将重点分析安全服务、安全机制及其相互关系。

1.2.1 安全服务

根据 ISO 7498 的定义,安全服务(security service)是指提供数据处理和数据传输安全性的方法。安全服务的功能是对抗安全攻击。ISO 7498 -2 定义了 5 种可选择的安全服务,如表 1-2-1 所示。

表 1-2-1 ISO 7498 -2 定义的安全服务

主要安全服务	子 类
认证	对等实体认证
	数据起源认证
访问控制	自主访问控制
	强制访问控制
数据机密性	连接机密性
	无连接机密性
	选择字段机密性
	业务流机密性
数据完整性	可恢复的连接完整性
	不可恢复的连接完整性
	选择字段的连接完整性
	无连接完整性
	选择字段的无连接完整性
非否认	数据起源的非否认
	传递过程的非否认

(1) 认证

认证(authentication)是为通信过程中的实体和数据来源提供鉴别服务。网络环境下的认证非常复杂，因为验证身份的双方一般都是通过网络而非直接交互。认证分为对等实体认证和数据起源认证。对等实体认证也称为身份认证，是指通信实体的一方认证另外一方的身份。数据起源认证是指数据的接收方证实所收到数据的发送方的身份。

(2) 访问控制

访问控制(access control)是保护受保护的资源不被非授权使用。访问控制可以控制不同用户对信息资源的访问权限，也可以防止授权用户滥用资源。对访问控制的要求主要包括一致性、统一性、可审计性和可控制性。一致性就是对信息资源的控制没有二义性，各种定义之间不冲突。统一性是对所有信息资源进行集中管理，安全策略统一贯彻。可审计性是对所有授权有记录并且可以核查。可控制性是指尽可能地提供细粒度的控制。访问控制可分为自主访问控制和强制访问控制。自主访问控制是指用户可以通过转让自己的访问控制权限，从而实现灵活的授权管理机制。强制访问控制是指系统由一个系统管理员实施权限管理，用户不能修改、转让自己的权限。

(3) 数据机密性

数据机密性(data confidentiality)是保护数据不被非授权泄露。数据机密性包括连接机密性、无连接机密性、选择字段机密性和业务流机密性。连接机密性是指为一次连接上的所有用户数据提供机密性保护。非连接机密性是指为单个无连接中的全部用户数据提供机密性保护。选择字段机密性是指为那些被选择的字段提供机密性保护，这些字段或处于连接的用户数据中，或为单个无连接中的字段。业务流机密性是指提供的保护使得通过观察通信业务流而不可能推断出其中的机密信息。数据加密(data encryption)是最常用的数据机密性保护手段。目前加密技术主要有两大类：一类是基于对称密钥的加密算法，也称为私钥算法；另一类是基于非对称密钥的加密算法，也称为公钥算法。如果从加密手段来看，一般分为软件加密和硬件加密两种。软件加密成本低，而且使用灵活，更换方便；硬件加密效率高，本身安全性高。可以根据不同需要采用不同的方法。

(4) 数据完整性

数据完整性(data integrity)是指确保接收方接收到的数据是发送方所发送的数据，且未被未授权篡改。破坏数据完整性的攻击行为包括修改、删除、插入、替换或重发。因此，数据完整性服务可保证合法用户接收和使用该数据的真实性。此外，数据完整性服务也可以在一定程度上提供对连接重放的检测功能。数据完整性包括可恢复的连接完整性、不可恢复的连接完整性、选择字段的连接完整性、无连接完整性和选择字段的无连接完整性。可恢复的连接完整性是指为连接上的所有用户数据提供完整性保护，并检测整个数据包序列中的数据是否遭到篡改、插入、删除破坏，同时进行补救或恢复。不可恢复的连接完整性与可恢复的连接完整性服务相同，只是不进行数据的补救或恢复。选择字段的连接完整性是指为在一次连接上传送的用户数据中的选择字段提供完整性保护，从而判断出这些被选字段是否遭受了篡改、插入、删除破坏或不可用攻击。

无连接完整性是指为单个无连接的数据包提供完整性保护,从而判断出一个接收到的数据包是否被篡改。选择字段的无连接完整性是指为单个无连接的数据包中的被选字段提供完整性保护,从而判断出被选字段的内容是否被篡改。

(5) 非否认

非否认(non - reputation)是指防止通信中的任一实体否认它过去执行的某个操作或者行为。具体来说,非否认要保证,当信息从发送方传递到接收方后,发送方不能否认这些信息是自己所发出的;如果确实收到了发送方所发送的信息,接收方不能否认自己没有收到。数字签名技术是实现非否认服务的主要方式之一。非否认包括数据起源的非否认和传递过程的非否认。数据起源的非否认是指为数据的接收者提供数据的"源发证据",从而防止发送者否认未发送过这些数据或否认其内容。传递过程的非否认是指为数据的发送者提供数据的"交付证据",以使接收者以后不能不承认收到过这些数据或否认其内容。

1.2.2 安全机制

安全机制(security mechanism)是保护信息与信息系统安全措施的总称。安全机制的内涵是检测、防御和恢复攻击的技术。ISO 开放系统互连安全体系中定义了 8 种安全机制,这些安全机制可以设置在适当的网络协议层上,以提供某些安全服务。

(1) 加密机制

加密(encipherment)机制既能为数据提供机密性,也能为通信业务流信息提供机密性,且还成为其他安全机制中的一部分,或起补充作用。常用的加密技术包括对称加密技术和非对称加密技术。

(2) 数字签名机制

数字签名(digital signature)机制至少包括两个过程:签名和验证。签名过程一般使用签名者所拥有的私有信息(如私钥进行操作),而在验证过程中,验证者需要使用公之于众的规程与信息(如公钥进行验证)。当然,验证者不能从这些公开信息中推断出签名者的私有信息。

(3) 访问控制机制

访问控制(access control)机制用于保护受保护的资源不被非授权使用。为了确定或实施一个实体对资源的访问权,访问控制机制可以使用该实体已鉴别的身份,或使用该实体的有关身份信息(如它与一个已知的实体集的从属关系),或使用该实体所拥有的权利。当实体试图使用非授权的资源,或以不正当方式滥用授权资源时,访问控制组件将拒绝这一企图,并产生一个报警信号或将其作为安全审计跟踪的一个部分记录下来,以供事后审计。

(4) 数据完整性机制

数据完整性(data integrity)机制包括单个数据单元或字段的完整性以及数据单元流或字段流的完整性两个方面。一般来说,用来提供这两种完整性服务的机制是不相同的。

(5) 认证交换机制

所谓认证交换(authentication exchange)机制,就是以在认证者和被认证者之间交换某些共享信息的方式来实现认证功能。可用于认证交换的技术包括以下几种:

① 使用鉴别信息,如口令,由发送实体提供,由接收实体验证。

② 密码技术,如公钥机制或对称密钥机制。

③ 使用该实体的特征或占有物,如认证令牌、指纹、虹膜等。

(6) 业务填充机制

业务填充(traffic padding)机制是指通过发送额外的数据来掩盖正常通信流量特征,从而达到保护业务流机密性的目的。业务填充机制能用来提供各种不同级别的保护,从而防止对业务流的分析。这种机制只有在业务流填充受到机密服务保护时才有效。

(7) 路由控制机制

路由控制(routing control)机制是指通过对路由过程进行控制,达到安全保护的目的。例如,多协议标签交换(MultiProtocol Label Switch,MPLS)就是路由控制机制的实现方式之一。

(8) 公正机制

公正(notarization)机制利用可信第三方来实现安全功能。公正机制建立在第三方公正的信誉基础上,通信中的所有实体必须完全信任该可信第三方。

1.2.3 安全服务与安全机制的关系

安全服务和安全机制虽然是截然不同的两个概念,但是两者联系紧密。具体而言,安全服务是由安全机制来实现的;一种安全机制可以实现一种或者多种安全服务;一种安全服务可以由一种或者多种安全机制来实现,如表 1-2-2 所示。

表 1-2-2 安全服务与安全机制的关系

安全服务 \ 安全机制		加密	数字签名	访问控制	数据完整性	认证交换	业务流填充	路由控制	公证
认证	对等实体认证	√	√			√			
	数据起源认证	√	√						
访问控制	自主访问控制			√					
	强制访问控制			√				√	
机密性	连接机密性	√						√	
	无连接机密性	√							
	选择字段机密性	√							
	业务流机密性	√					√	√	

续表

安全服务 \ 安全机制		加密	数字签名	访问控制	数据完整性	认证交换	业务流填充	路由控制	公证
完整性	可恢复的连接完整性	√			√				
	不可恢复的连接完整性	√			√				
	选择字段的连接完整性	√			√				
	无连接完整性	√	√		√				
	选择字段的无连接完整性	√	√		√				
非否认	数据起源的非否认		√		√				√
	传递过程的非否认		√		√				√

注:其中√表示对应的安全机制(行)可以实现对应的安全服务(列)

1.3 安全服务的分层部署与实现

国际标准化组织(ISO)在开放系统互连标准中定义了包含7个层次的网络互连参考模型,分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层,如图1-3-1所示。不同的层次提供不同的功能,例如数据链路层负责建立点到点的通信,网络层负责路由,传输层负责建立端到端的通信信道。

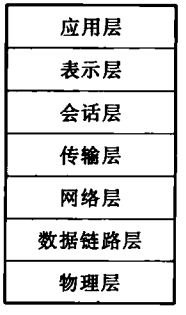

图1-3-1 OSI模型

相应地,在各层可以根据不同的需要实现不同的安全机制,从而实现不同的安全服务,表1-3-1是各种安全服务在OSI模型中的分层部署实现情况。