网络与信息安全技术丛书

语音与数据安全

（美） Kevin Archer 等著

王 堃 周 毅 章 颖 等译

机械工业出版社
China Machine Press

本书介绍电话网络安全和数据网络安全，以及相关的协议和安全技术。主要内容包括：两种网络一体化方面的基本知识，当今网络环境的安全观念，传统电话网络及其组成元素的安全隐患，最新集成网络的安全隐患，传统的安全主题等。本书内容覆盖面广，分析透彻，是语音技术应用开发人员的实用参考书。

本书版权登记号：图字：01-2001-4292

图书在版编目（CIP）数据

语音与数据安全/（美）阿切尔（Archer, K.）等著；王堃等译. -北京：机械工业出版社，2002.7

（网络与信息安全技术丛书）

书名原文：Voice and Data Security

ISBN 7-111-10284-3

Ⅰ.语… Ⅱ.①阿… ②王… Ⅲ.计算机网络-安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2002）第030842号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：刘 晖 周 睿

北京第二外国语学院印刷厂印刷·新华书店北京发行所发行

2002年7月第1版第1次印刷

787mm × 1092mm 1/16 · 18.75印张

印数：0 001-4 000册

定价：35.00元

译 者 序

在因特网大行其道的今天，各个公司纷纷建立起自己的数据网络。面对网络一体化的趋势，人们必须重新认识语音和数据网络的关系，才能够充分利用其所蕴含的网络资源。然而在利用资源的同时，人们更应该注意其潜在的危险性——水能载舟，亦能覆舟。面对众多各具破坏力的“杀手”——黑客，如何才能确保网络数据的安全性呢？这正是我们翻译本书的动机。本书作者在系统地分析了各种网络数据安全问题的基础之上提出了详细的解决方案，对组建各种网络系统的人员具有很高的参考价值。

书中的第一部分对有关网络安全的基本知识和术语进行了科学准确的介绍，为初学者学习后面的章节打下了必要的理论基础。第二部分详细介绍了当前威胁网络安全的主要因素及具体的预防措施。第三部分介绍了传统的电话网络及其组成元素的安全隐患，并为读者介绍了大部分机构采用的另一种工具——语音邮件系统。第四部分介绍了最新的集成网络的隐患，并对前面介绍的协议开发方法和语音、数据传输技术进行了进一步的讨论。和其他同类的书籍相比，第五部分介绍了更多的传统的安全主题，同时还介绍了由于20世纪后期的几件重大事件而备受关注的新主题，如拒绝服务攻击、网页安全、宽带安全、安全出口和各种法案。本书既包括电话网络又包括数据网络，对于在这两个领域没有经验而又对此感兴趣的朋友们，本书是您的最佳选择。

本书第一部分由王堃翻译，第二部分由周毅翻译，第三部分由章颖、张晓哲翻译，第四部分由王俊伟、刘侃翻译，第五部分由赵锋、李铭翻译，全书由朱珂审校。

由于译者水平有限，书中难免有不当之处，敬请读者指正。

2002年4月

前　言

在20世纪90年代后期的信息技术领域中，最热门的话题是对语音和数据网络的集成。这种集成虽然在多年前就已出现，但直到IP语音业务（VoIP）和网络语音(VoN)的引入，这种集成才得到突破性的进展。本书涵盖了电话网络安全和数据网络安全两大主题，随着这两种网络一体化的发展进程，随之而来的安全问题也需进一步解决，另外，还要关注众多相关协议的安全及技术方面的安全，这些内容在本书中都有详细的介绍。

本书分为以下几个部分：

第一部分　背景

这部分内容阐述了以后各章需要用到的关于安全、网络和一体化方面的基本知识，通过这部分的学习，为以后进一步学习网络安全方面的知识打下基础，已经有一定基础的读者，可以直接从第5章开始学习，你会体会到本书对数据、语音和可视网络管理者的重要意义。第6章将进一步探讨这一主题，讨论现今各机构网络的构成，该部分最后两章将为读者介绍网络语音业务传送的基本方法。

第二部分　保护数据网络免受基于Telco的攻击

这部分内容系统地阐述了当今网络环境的安全观念，虽然人们几年前就对电话网络给数据网络带来的安全威胁了然于胸，但至今也没有对这种威胁做出过具体的阐述。第9章探讨了多年来使用的电话连接给数据网络带来的威胁的解决方法，这种方法对人为制定的安全策略具有严重的依赖性，整个计算机安全的发展史也证明了仅靠方法是难以奏效的，第9章中提到的装置虽然不能解决modem带来的问题，但它们却能提供重要而实用的功能。第10章则介绍了专门解决modem产生的问题的新技术——通信防火墙，和它的姊妹产品数据防火墙一样，通信防火墙能够解决PBX系统的安全隐患。

第三部分　保护语音安全有效

这部分内容介绍了传统的电话网络及其组成元素的安全隐患。第12章介绍了开发当今众多机构中的普通PBX的方法。第13章为读者介绍了一种现在已经广为所用的新科技，该部分最后还为读者介绍了大多数机构采用的另外一种工具——语音邮件系统。

第四部分　网络和多媒体服务的语音防护

这部分内容介绍了最新集成网络的安全隐患，并就前面介绍过的协议开发方法和语音、数据传输技术进行了进一步的讨论。安全问题并不是集成环境中惟一的讨论对象，有时候其他因素会比安全问题更重要，第15章详细介绍了这些因素。第16章讨论了在传载语音的多种媒体中存在的各种安全问题。在一体化的环境下，语音和计算机数据并不是惟一传送的信息。第17章介绍了与

语音和计算机数据并存的其他类型的数据以及相关的安全问题。

第五部分　数据网络安全问题

与其他关于计算机安全和网络安全的书相比，这部分内容介绍了更多的传统安全主题，为读者展现了一幅完整的安全画面，对基础网络安全较为熟悉的读者在阅读这部分时没有必要花费太多的时间。本部分各章均独立于其他章节，所以你可以单独阅读其中一章。本部分内容涉及加密技术、防火墙、入侵探测、检测、扫描、密码破解和恶意软件，并收入了由于20世纪后期的几件重大事件而引发的倍受关注的主题，如拒绝服务攻击、网页安全、宽带安全、安全出口和各种法案。

为满足读者对相关内容的进一步了解，本书列出了参考书目。另外，本书英文版出版社网址http://www.samspublishing.com/中有本书讨论过的各种工具的链接，欢迎登录该网站查找最新信息。

本书读者

本书是为工作在数据网络系统和电话网络系统中的朋友们编写的，人们会越来越清楚地看到这两种网络一体化带来的安全问题是多么的重要，当然，对安全问题感兴趣的朋友也可以阅读本书。

由于本书既包括电话网络又包括数据网络，所以对这两个领域没有经验而又感兴趣的朋友，本书是您的最佳选择，随着社会对安全人才的需求越来越迫切，会有越来越多的朋友想加入到对有关安全方面的知识的学习中来，对他们而言，本书也是一本新的最佳入门教材。

虽然本书是为电话网络和数据网络方面的科技人才编写的，但由于本书提供了详细的基础背景资料，所以管理者也可阅读本书。随着各个工作岗位科技含量的不断提高，管理者需要对商业运行所依靠的科技基础有越来越深入的了解，对于从事管理工作的读者们，作者建议仔细学习完第一部分后，再学习后面的章节。

最后，对计算机和网络安全感兴趣的老师和学生既可把本书作为学习计算机和网络安全的入门教材，也可作为学习其他安全教程的补充教材，因为本书不是作为教材而编写的，老师们可以根据自己的需要和具体情况补充必要的章节。

本书英文版原书书名：Voice and Data Security
本书英文版原书书号：ISBN 0-672-32150-5
本书原出版社网址：www.samspublishing.com

作者简介

Gregory B. White，PH.D原是一名空军。作为美国科罗拉多州斯普林斯空军学院计算机科学部的带头人，他工作了整整19年，在学院工作期间，他一直致力于计算机安全和信息战这两个方面的研究，并力图使计算机安全教育贯穿于整个计算机科学教育课程中，在这期间，他就计算机安全和信息战写了大量的著作，他还是两本计算机安全教科书的作者之一。

在空军学院的指派下，White在得克萨斯A&M大学学习了三年并获计算机博士学位，他的研究课题是基于主机和网络的入侵检测。他还兼任得克萨斯州圣安东尼奥中心网络安全部门主管，他在空军学院的第一个职务就是担任奥马哈Nebraka空军战略指挥司令部的系统分析专家。

White博士现在负责空军部信息防御系统的工作，并在位于圣安东尼奥的得克萨斯大学教授计算机安全课程。

White博士于1995年在得克萨斯A&M大学获得计算机科学博士学位，1986年在空军科技研究所获得计算机工程硕士学位。1980年从Brigham Young大学获得计算机科学学士学位。

Dwayne Williams拥有Beylor大学的计算机科学学士学位，现任Securelogix公司的专业指导设计师，该公司向广大用户提供新型安全和集成产品，TeleWall防火墙就是其中之一。

Williams先生主要负责指导和管理有关数据网络和远程通信网络安全方面的服务咨询，包括评估服务、安全体系结构设计和安全操作方式等多项任务，在加入Securelogix公司之前，他在美国空军部任通信系统和计算机系统官员达6年，曾受聘为第609信息站小分队的工程技术领导。

Kevin T. Archer在网络和计算机安全方面有5年多的工作经验，特别是在Cisco路由器和转换器方面，更有独到的贡献。他曾经为ISP开发和实现过国际卫星与地面通信的连接，并有着为财富500客户作受控穿透测试的经历。Archer先生持有CCNA和MCP证书，他目前在Securelogix公司担任高级网络安全工程师，他的基本工作是负责受控穿透性测试、产品评估和数据检测。

James D. Core在Indiana and Vincennes 大学获得远程通信学位，2000年9月到2001年4月，他在SecureLogix公司任高级电信工程师，他现任俄亥俄BMW计算机电话学工程师。在加入Securelogix公司以前，他还曾在得克萨斯的Norwest银行和EDS任语音网络工程师。

Chuck Cothren在信息技术和信息安全方面有5年多的工作经验，尤其擅长网络设计和管理，它的经验包括网络操作中心设计和实施、网络管理、可控穿透性测试和系统管理。现在他受聘为Securelogix公司的网络安全工程师，Cothren先生拥有得克萨斯A&M大学的理学学士学位，他是拥有微软证书的系统工程师和拥有Nortel Networks证书的专家。

Roger L. Davis拥有乔治华盛顿大学的计算机学硕士学位和Brigham Young大学的计算机学士学位，他在科罗拉多大学完成了他的研究生学业，他是作为一名高级安全工程师于2000年6月加入Securelogix公司的，他与他的同事们一起为主要的商业集团和大的研究所进行风险评估，他是一名退役军人，有着20多年军旅生涯的Dewis先生退役时是空军中校。服役期间，他曾创建了24小时空间指挥中心来帮助美国空军指挥部的首脑，在全球定位系统和空军全球化卫星控制网

络中占据了主要地位，他曾在Brigham Yong大学和空军技术研究所教授本科和研究生课程，并参加过包括IEEE精确定位和航行专家会议在内的多次工程及会议。

David J. DiCenso拥有Maine大学的商业管理和经营学学士学位及Vermont法律学校的法学博士学位，目前他正在San Antonio地区进行法律实践。

他于1999年3月至2001年1月担任SecureLogix公司的训练服务部主管，在此之前，他作为美国空军法律代理工作了11年，精通刑法、民法等多种法律，在美国空军科学院执教期间，获得了学院副教授头衔，他现为AF服务部少校，分配到Kelly FAFB的空中智能机构工作。

DiCenso先生为美国空军学院的法律教科书作了前言，出版了有关Cyberlaw和信息战方面的书籍：《Airpower Journal》（空军力量征程）和《World Jurist Association's Law/Technology》（世界法学家协会原则）。这些经历和研究工作给他带来了机会，包括DEFCON2000和IDTV'S C项目在内。他随后还参与了许多项目的研究。

Travis J. Good现任SecureLogix公司的高级网络安全工程师，他现在的主要工作是为财富500客户做可控穿透性测试和其他相关安全问题的研究工作。在加入SecureLogix公司之前，他在包括电子商务在内的IT领域工作。

目　录

第五部分 数据网络安全问题

第一部分 背 景

第1章 网络安全隐患

主要内容：

- 风险波及的范围有多大
- 各种各样的安全威胁
- 脆弱性
- 使网络更安全的推动力

“大学者们对信用卡黑客攻击束手无策”——2D网站消息

“到处进行破坏活动的‘Serb黑客’”——BBC消息

“美国政府报告公布计算机安全威胁的情况”——网络日报

诸如此类的新闻标题曾极少出现在媒体报导中，三十年前，计算机安全问题只与少数人有关，而计算机互连只是科幻故事中才有的概念。而今天，如果想在一周内听不见也看不到计算机安全或者与之相关的媒体报道，也算是一件十分困难的事。

计算机虽不如电话这样普及，但也已经非常普遍。几乎没有什么事能离开计算机而顺利进行。网络通过通信手段将千家万户联系起来，它已成为客户与客户，公司与公司，以及公司与客户之间进行交易的一种主要商业渠道了。如今，很多人花钱在家中安装了高速的数据通信线路，这样，人们就可以更方便、更快速地穿梭于信息高速公路上了。

尽管大部分人愿意遵守专为这个数字领域所制定的规则，但仍有一些人试图逃避已经实施的安全监控与保护，一旦这些人得逞，我们便会看到上文所提到的新闻报道。也正是由于这些人的不法行为，才使得类似于本书的各种书籍变得必不可少，因为人们想保护自己及其各种绝密信息不受非法入侵者的威胁。

保护我们的信息系统，使之不受各种威胁，这些威胁通常通过各种连接来侵害我们的数据和电话网。这并不是一件不花任何代价就可做到的事。当你花费了大量金钱，安装了昂贵的安全监控设备来保护系统及各类数据的同时，你每天还得做许多妥协和让步，比如风险、潜在损失、对个人机密文件以及用户社区的冲击，这些都必须考虑进来，以确定实施这种安全举措是否划算。那么，对系统和数据的威胁都有哪些呢？这种风险所波及的范围有多大呢？你的计算机系统被入侵遭破坏的可能性有多大？这一章将介绍各式各样的对数据和电话网的威胁。第2章“安全要素”，将讲述基本的安全原则，并介绍一些与计算机安全有关的基本概念。

1.1 风险波及的范围有多大

计算机安全研究所（CIS）和联邦调查局（FBI）每年都会联合进行一次民意调查，以确定

安全问题在行业及政府部门中所涉及的范围有多广。《信息安全杂志》每年也会做同样一个民意调查。这两份调查结果及一些普通的调查都表明，对于某个组织机构的网络系统，其最大的威胁来自于该组织的内部——职员、临时雇员或别的获权留在该组织的人员（比如保管人员）。

20世纪后期，《信息安全》杂志的调查结果显示，有52%的被调查人有过职员滥用计算机访问控制的现象（即，用户试图执行他们未被授权的操作），这个数字在新千年开始又上升至58%。同时，在接受调查的人当中，只有1/4的人报告说有外部人员越权访问的现象。

CIS/FBI的调查也显示出同样的结果，55%的越权访问系内部人员所为，而只有30%的系统入侵行为为外部人员所为。一年后，该调查报告显示的情况更为糟糕，约有71%的越权访问为内部人员所为，而只有25%的系统入侵来自外部人员（在上报的事件中，有27%怀疑属于服务攻击）。

但是，这两份民意调查的结果也许并不能代表大多数的现象。因为接受《信息安全杂志》调查的人是该杂志的读者，而接受CIS/FBI调查的人则是从事计算机安全的人。你可能会争辩，这些人比普通的民众了解的安全知识多得多。将所有的人都包括进来，计算一下行业及政府部门中这类现象的发生率到底有多高，这的确是一件很有趣的事。

根据这些民意调查显示的结果，我们发现最大的安全问题是由病毒引发的。这些年来，病毒（以及其网络兄弟蠕虫）引发的问题逐渐增多，事实上，许多罪行极其严重的计算机安全犯罪都与病毒和蠕虫有关，其中经济损失最为严重的是2000年5月份发生的情书（或爱虫）病毒。一名叫Onel. de Guzman的菲律宾学生，被控告发布了这种病毒的代码，使成千上万的计算机系统受到病毒感染，导致行业及政府部门的计算机出现停机故障，从而损失了上十亿美元。最近一次的《信息安全杂志》的民意调查显示，80%的被调查人所上报的安全问题与病毒、特洛伊木马及蠕虫有关。而此前的两次调查结果分别73%和78%。

由于计算机安全遭破坏而带来的经济损失也在逐年上升。通常情况下，我们很难确定这种损失到底有多大，但据1999年度《信息安全杂志》所进行的民意调查结果显示，每次破坏事件平均约损失256 296美元。同年CIS/FBI的调查报告所列的经济损失数额几乎是《信息安全杂志》所列数额的三倍之多，每次平均约损失759 380美元，这个数额到2000年又增至972 857美元。

有趣的是，这些数字存在着极大的不一致，这主要是因为很难确定如何计算每次破坏所造成的经济损失及应该考虑哪些因素。

很多人认为，管理者在破坏事件发生之后用于恢复系统的时间应算做计算机被入侵所造成的损失。重装操作系统、恢复备份数据、重新编译实用程序及其他程序、删除越权账户和恢复网页都是系统被入侵后所必须做的工作，而完成这些任务所花费的时间完全可以算做与入侵直接有关的劳动时间。

有人说，用于安装安全补丁的时间不应该加入计算入侵所造成的经济损失中，尽管这种补丁可以抑制计算机发生外来入侵的脆弱性，但这项工作无论什么时候都必须做。而实际上仍有人会反驳说，如果这些安全补丁早已安装好的话，系统根本不会被外来入侵破坏。

对于其他一些因素是否该加入计算入侵所造成的损失中，很少有人有异议。比如，被窃取的软件和信息的价值。通常情况下，由于执法部门和法官有意要将经济损失最大化以造成对被告不利的形势，他们通常强烈要求将这些被窃取的软件和信息的价值列入经济损失当中。这种

计算应该取决于软件本身的价值。如果该软件已在市场上出售，其价值就应以零售价计算。如果该软件尚处于开发当中，或它只是公司的私有财产，不在市场上出售的话，问题就不那么简单了。以前类似于这样的例子不少，检察官们试图用开发软件所花费的成本来确定经济损失。这种计算方法所得出的数字常为各大媒体引用，因为这些数字常以上万美元出现，不过，它们一般不会出现在法庭审判当中。

由于信息丢失，计算机和网络无法运行，人们不能正常工作，从而影响了生产率，与此对应的时间损失也常被加入到经济损失的计算公式中。如果加上损失的生产率及事后用于清理系统的时间，20世纪末几次较大规模的涉及病毒和蠕虫的事件造成的经济损失，可以达到上亿美元。

其实，入侵者所攻击的目标不仅仅是计算机系统及数据网络。同样的民意调查显示，专用的电信通信安全工程也常常成为黑客们入侵攻击的目标。在接受调查的人当中，有超过10%的人说，他们的电话网、专用交换机和语音信箱系统曾遭入侵袭击。而军队和教育部门的计算机系统遭侵袭的比例更高，约有四分之一的被调查者说他们的系统被入侵过。

1.2 各种各样的安全威胁

对计算机系统，网络和电话通信设备的威胁有各种形式。自然灾害，如龙卷风、暴风雪、尤其是电子风暴，给电子设备造成了毁灭性的破坏。火灾、浓烟、自动洒水器和灭火设备也会带来严重威胁。这些威胁大都源于自然灾害，并且对任何昂贵的电器装置都有巨大的破坏作用。（比如电视机、录相机、立体声设备、X射线机器等等）。因此，除提醒读者要使用一个运行程序定期备份一些敏感重要的数据、软件，以便将其储存于另一个独立的程序中外，本书将不再花太多笔墨讲述这个问题。

1.2.1 内部威胁

具体地说来，对数据、电话网及通信设备的威胁可分两大类：内部威胁及外部威胁。如我们先前所提到过的，来自外部的入侵和攻击往往占据了媒体新闻标题的大部分空间。而事实上，大多数的问题是由于工作人员滥用计算机系统而产生的。内部人员知道那些最重要的数据存放在什么地方，也能访问程序及设备，他们有足够的时间，可以谨慎耐心地行事，因此通常不易被察觉和怀疑。有趣的是，在政府部门中，一个称职出色的公务员和一个间谍的特征竟是一样的（比如，勤奋、自愿做额外的工作、常加班加点、很少休假等等）。这一点，可以帮助我们解释为什么那些内部的不法分子常常难以被发现。

1. 安全漏洞

内部的威胁也以各种形式出现，它们并非全都是蓄意的。其中，最重要的威胁之一就是那些没有经过严格培训的操作人员。众所周知，大部分的入侵行为正是由于系统配置不合理或是没有执行安全策略而引起的。

举个例子，其中一个最大的问题就与登录口令和写密保护有关。每年，都有许多由于用户选择了过于简单的口令而引起安全破坏的事件发生。然而，只要用户按照所制定的规则选择登录口令及写密保护，这种问题是完全可以避免的。

如果管理员没有安装最新的操作系统补丁，也常会发生安全破坏问题。不管是因为缺乏时

间或对安全补丁的重要性的培训，入侵者都有机可乘，不断地找到安全漏洞。（通常这时入侵者对那些尚未发现或刚刚发现到的漏洞无可奈何。但是如果系统管理员早已安装了安全补丁，那么任何已知的安全漏洞都不会被入侵者所利用。）

有非常重要的一点我们必须加以区别，就是这些没有经过严格培训的内部人员与那些滥用系统权限或企图破坏系统的内部人员是不同的。但是，他们的行为会给妄图入侵系统进行破坏活动的不法分子提供便利。这一点同样适用于我们将要介绍的另一种内部威胁，他们对所制定的安全规则视而不顾。

在此我们要引用一个典型的案例：一个职员用调制解调器连到其他办公室的电脑上，以便通过拨号可远距离地操纵计算机继续工作。这个职员并非想闯入计算机系统或通过越权访问来进入计算机系统，但他的行为却给其他外部人员非法获得该组织计算机系统的访问权提供了便利。这个未授权的调制调器就是问题的症结所在。职员将它与计算机系统联接起来本是出于一个很好的目的——他想继续工作，但不幸的是，别人也可以通过这个调制解调器获得进入该组织的访问权。这项被外来入侵者利用的技术其实很简单，他只需拨一下电话号码直到与调制解调器相连的计算机作出回复，他的其他目的便可马上达到了。这项技术有一个专业的名称，叫战争拨号。我们将在下一章里详细讨论。

2. 蓄意威胁

那些心术不正，企图逃脱安全监控的内部人员，对系统的安全威胁更多更大。这类人大致可分两种：第一种是潜伏在政府部门或企事业单位内部的从事间谍活动的人。像上文提到的调制解调器案例，政府和企业内部的间谍就有可能将调制解调器连接到他所服务的组织机构的一台机器上，这样他就能通过拨号给另一个政府或企业传送机密情报和文件了。这种人会试图努力提高自己的授权级别或获得其他系统的访问权，以便能访问到该组织存放在别处的绝密文件。这类人通常很难被发现，因为他们通常被认为是出色的值得信赖的雇员。即使事情败露，他们通常也只会得到一点口头的训斥，因为该组织机构的高层人士认为他是一名有能力的职员。

像这种内部人员带来的潜在破坏，还有一个很好的例证，即Guillermo Gaede案件。1996年，这名阿根廷籍公民在承认自己窃取了英特尔公司生产奔腾芯片的生产技术相关绝密信息后，被判入联邦监狱33个月。在英特尔公司设在Arizona的Chandler设备厂工作期间，Guillermo窃取了这份信息，事后不久也就是1993年他逃到了阿根廷。在那儿他把这份绝密信息寄给了AMD公司，该公司是英特尔公司的一个竞争对手，也是他从1979年到1992一直为其工作的公司。AMD马上与FBI取得联系，并将这份文件寄给了FBI。在不久后Guillermo返回美国时，FBI逮捕了他。Guillermo通过一个调制解调器在家访问到了一些绝密敏感的数据，然后当计算机屏幕显示这些重要的信息内容时，他就用录像带将它拍摄下来。“Gaede挫败了这个由一个非常清醒的安全制造商制作的安全监控系统。”美国国家律师事务办公室的一名主要负责人，Leland Altschuler在California的San Jose这样说。这个例子证明了要想保护信息不受内部入侵者的破坏是多么困难。

第二种蓄意入侵的内部人员是那些对公司或本组织不满或已被解雇的职员。由于各种原因，这类人想方设法企图破坏该组织。正如那些商业间谍一样，这些对组织不满的职员通常知道组织内部的绝密数据和文件存放在什么地方，他们知道什么能带给该组织巨大的损失。有时，他