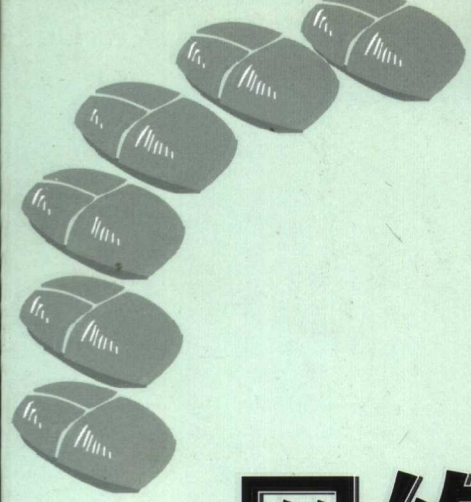
高等院校计算机教育系列教材

# 计算机网络安全与管理

李　卫　等编著



清华大学出版社

高等院校计算机教育系列教材

# 计算机网络安全与管理

李　卫　编著

清华大学出版社

# 内 容 简 介

本书针对计算机学科的特点，主要介绍加密算法在该领域的基本实现和应用。书中不过多讲述原理，而是在综合介绍各种网络攻击和防范技术的基础上，进一步强调如何用动态的手段来解决动态发展的网络安全问题。所应用的管理手段包括对设备、技术、人员、业务等各个方面的管理。

全书共分8章，内容包括常见的各种加密算法以及应用，常见的各种网络攻击原理及防护手段等，并强调网络安全的动态发展这一特性，全面阐述了如何从管理的角度出发，结合不同的技术手段，解决各种网络安全问题。

本书适合于计算机、通信等专业高年级本专科生及研究生作为教材使用，同时也可以作为工程技术人员的技术参考书。



**图书在版编目(CIP)数据**

计算机网络安全与管理/李卫编著. —北京：清华大学出版社，2004.11

(高等院校计算机教育系列教材)

ISBN 7-302-09515-9

Ⅰ.计…　Ⅱ.李…　Ⅲ.①计算机网络—安全技术—高等学校—教材②计算机网络—管理—高等学校—教材　Ⅳ.TP393.0

中国版本图书馆CIP数据核字(2004)第094179号

**出 版 者**：清华大学出版社　　**地　　址**：北京清华大学学研大厦

http://www.tup.com.cn　**邮　　编**：100084

**社 总 机**：010-62770175　**客户服务**：010-62776969

**组稿编辑**：邹　杰

**文稿编辑**：葛昊晗

**封面设计**：陈刘源

**印 刷 者**：北京市世界知识印刷厂

**装 订 者**：三河市金元装订厂

**发 行 者**：新华书店总店北京发行所

**开　　本**：185×260　**印张**：23.25　**字数**：552千字

**版　　次**：2004年11月第1版　2004年11月第1次印刷

**书　　号**：ISBN 7-302-09515-9/TP·6619

**印　　数**：1～5000

**定　　价**：33.00元

# 序　言

计算机网络安全是一个随着互联网的发展而不断引起人们关注的课题。虽然目前“安全”、“黑客”已经成为众所周知的名词，但人们对于安全的理解仍然存在着一些误区。

一个误区是认为联网是一件很不安全的事情，乃至在网络上什么应用都不敢使用，如购物、交友等。其实，正如在现实生活中一样，我们随时也可能会遭遇交通、疾病、偷窃等风险，可我们还是要照常生活。安全的风险在任何地方都是存在的，关键在于我们如何去减小它。本书的目的之一，就是说明如何通过各种网络安全技术和安全管理措施来最大限度地减少网络安全的风险。

另一个误区是认为网络安全只是专业人员的事情，或者网络安全只需要采用一些安全产品、安全技术就可以了。这也同现实生活一样，安全不只是警察的职责，还需要社区、个人等多方面的积极参与。同时还应当认识到，安全也并不是买一个好的防盗门、好报警器就可以解决的问题。

还有些人认为，自己的机器、系统、网络安全了就足够了，这是一种狭义的安全观念。事实上，如果别人的系统不安全，自己也会受到很大的影响，在网络的世界中谁都不能保证独善其身。

本教材是作者在整理、收集网络安全方面各种有关的资料，并结合自身的教学、科研和网络运行管理经验的基础上编著的。除了引用了一些组织如 IETF、NIST、ITU、ISO 等的有关标准外，还引用了一些“黑客”攻击的“反面教材”，力图从攻击者、网络用户、网络管理者等几个角度来阐述网络安全问题。

值得说明的是，虽然本教材用了很多篇幅来说明网络安全中涉及到的各种技术，但贯穿始终的思想是网络安全不仅是一个技术问题，更是一个人的观念问题。网络虚拟社会的安全就是现实社会安全的一个映射，只要现实社会中的安全问题存在，网络安全问题就会一直存在下去。

透过各种专业名词，我们所看到的实际上是人与人的对抗，因为任何技术的进步对于攻击者和防守者都是同样受益的。从远古到现在，在技术进步的外表下，这种对抗的本质是没有发生什么变化的。这就如同锁的发展，从古代很简陋的锁，到今天采用了非常复杂技术的锁。然而，偷盗问题是一直存在的，对抗的水平发生了变化，对抗却从来没有停止过。

因此，没有任何网络安全技术和产品可以保证网络的绝对安全。网络安全需要“三分技术，七分管理”，这是有一定道理的。解决网络安全问题不仅需要更多的安全产品和技术，也需要管理措施。只把注意力放在寻找万能的技术灵丹妙药上是靠不住的，而建立完善的安全管理，虽然需要很多资源，却是更为现实可行的办法。

本教材涉及到了较多的计算机专业基础知识，如操作系统、网络原理、程序设计等。本书既可以作为计算机专业高年级学生的教科书，也可以作为其他相关专业学生的参考

书目。

本书在内容上分为 8 章：

第 1 章“网络安全概述”，主要介绍了当前网络安全领域发展的现状，网络安全要解决的核心问题，以及目前从事网络安全防护研究的部分著名组织和机构。

第 2 章“攻击”，主要说明攻击者如何利用各种手段(技术和非技术的)，通过本地或者网络，对目标进行攻击。本章也说明了网络结构、协议、软件、操作等方面的缺陷或疏忽如何导致了攻击的发生。

第 3 章“密码技术”，主要对构成网络安全基本防护技术的常见加密算法及其应用，如认证、数字签名等进行了说明，使得读者对密码技术有一个基本的了解。

第 4 章“密钥管理及证书”，说明在加密算法的应用中，除了算法本身的安全性外，密钥管理的重要性以及如何实现密钥管理。

第 5 章“安全应用及协议”，主要说明 IETF 及其他机构针对 Internet 各个主要协议，在安全方面的改进和加强。本章除了讨论协议外，还涉及到很多加密技术的应用。

第 6 章“安全访问控制”，主要说明在操作系统、网络中，如何实现对资源访问的有效控制，以及如何对访问进行监控，如何提高安全水平。

第 7 章“安全设备管理”，在传统网络管理的基础上，说明对安全设备进行管理所出现的新问题，以及现有的解决方法。

第 8 章“安全管理”，主要说明如何通过人员、操作流程，结合技术手段，实现对网络的动态安全管理。其核心不仅是管理的方法，还包括其主导思想，即有专业人员不断参与的动态管理流程是实现网络安全的最佳保证。

附录介绍了一些背景知识，如数论、AT&T 汇编指令、Linux 环境下的程序设计、部分攻击代码、实验 PKI 的建立等。

由于本书涉及到的技术领域较广，而编写的时间很紧，因此无论在结构还是在内容方面，都有许多不尽人意的地方，欢迎读者批评指正。

在本教材的编写过程中，韩博、刘小刚、林海等整理了附录中的部分资料，在此表示感谢。

编 者

# 目　录

# 第 1 章　网络安全概述

## 1.1　网络安全现状

提到网络中的安全问题，以前很多人会认为这是军事领域的事情。但 Internet 的商业化迅速改变了这一切，不仅使得网络安全成为一个引人注目的话题，也成为目前信息领域研究中最热门的技术之一。从电子邮件到移动电话，从网站访问到数字现金，网络中的每个活动都离不开网络安全。

随着网络的普及以及网络应用的发展，人们对计算机网络的依赖程度日渐加深。网络安全不仅对每个人都有现实意义，对于一个国家国民经济的正常运转、国家安全等，也都比以往有了更密切的关系。由于网络信息安全所导致的问题，已经给企业、政府部门、金融公司等造成了重大损失。

我们可以把网络安全问题看成是现实社会中安全问题在网络上的一个映射，或者影像，现实生活中具有的各种问题在网络上同样会存在。例如，现实生活中所有的交易都有遭受诈骗的风险，如假化肥、假钞票、假发票等；同样，电子交易也会遭受各种攻击，如假冒身份、虚假信息、拒绝服务等。

不同的是，由于网络所具有的一些特性，如开放性、匿名性，以及网络技术的不断发展等原因，在网络上通过计算机进行攻击要比现实中更容易。在网络中要伪装成另一个人也比现实生活中要容易得多，而隐私却更难保护。

例如，一旦电子邮件地址被某些人获取后，随之而来的就是大量的垃圾邮件，但收信人几乎无能为力，因为发信人可以不断更改自己的地址、标题，并对内容做一些变动。任何一个用户，都可能遭受到内部人员或者全世界各个地方不怀好意的攻击者的攻击。在计算机紧急响应小组(CERT)的年度报告中，列出了 2002 年发生的将近 80 000 多个有报道的安全事件，其影响涉及到将近 440 万个 Internet 主机。

对于各个公司来说，尽量保护网络安全是必然的选择。例如，欧洲国家法律规定公司有责任保护其客户的隐私，美国政府对于银行、医疗等行业也有类似的规定。如果公司提供的业务不能保证，则要承担相应的法律责任。因此，很多机构除了使网络更安全外，几乎别无选择，这也是网络安全格外重要的原因。

安全问题由来已久，但又随着其他技术，如通信、计算机网络等技术的发展而不断产生新的问题。安全问题是一个综合学科的技术，涉及到数学、计算机、通信、管理、法律等多个领域。虽然从不同学科的角度出发，都有不同的解决办法，但任何一种单一的方法都不能完全解决网络安全问题，因此，它是一个综合学科的问题。

在网络安全中，“黑客”是个经常出现的词汇，源于英语中的“hacker”，本意是指一些计算机水平很高的程序员，可以发现系统中潜在的漏洞，他们可能彼此之间经常互相

交换安全信息，但从不蓄意破坏计算机系统。

例如，比较著名的“黑客”有：

- 建立自由软件基金的 Richard Stallman；
- 开发 MS-DOS、Windows 等的 Bill Gates 和 Paul Allen；
- 开发出 C 语言及 UNIX 操作系统的 Dennis Ritchie、Ken Thompson 和 Brian Kernighan；
- 开发计算机口令及安全系统(COPS)的 Eugene Spafford；
- 开发 SATAN 和 TCP Wrapper 的 Wietse Venema；
- 开发 Linux 的 Linus Torvalds。

而未经授权进入别人的系统，并具有恶意的人，如对数据进行篡改、删除，或者破坏系统，非法获取信息等，则称为破坏者(cracker)。比较著名的有 Kevin Mitnik、Kevin Poulsen、Justin Tanner Peterson 等。他们对电话系统进行攻击；成功进入了许多军事、金融、软件公司的计算机系统；对信用卡进行窃取等。这些攻击活动造成了很大的损失。

现在的网络安全情况又和 Internet 发展早期有所不同。由于网络的普及，以及各种攻击工具容易获得等原因，即使是一个初学者，也可以轻易对计算机系统进行攻击。尽管目前采取了安全防护措施的机器比以前多了，但是，具有安全漏洞的机器也比以往更多了，这包括一些家庭用户、非专业人员的机器等。在 5 年前，拒绝服务、漏洞、后门等还是少数人了解的词汇，现在已经成为报刊新闻中的常用词了。

网络攻击的动机则非常多样化，在很多情况下是机会主义的：

- 有些人只是为了获得知名度，他们拥有很多的资源(时间、计算资源、金钱等)，不断地寻找目标，进行各种尝试攻击；
- 电子流氓没有明确的目标，可能会入侵不同的系统，篡改网页，发送大量的垃圾信息；
- 网络安全的研究者、执法者为了证明一个计算机系统是不安全的，也需要模拟攻击；
- 政府则成立了专门的“网络军队”，进行网络的攻防战。

因此，在今天，“黑客”已经失去其早期“技术高手”的含义，而成为任何进行攻击活动的人的代名词。我们在本书中，把那些进行非授权访问、修改数据，或使系统不可靠、不可用的活动称为攻击活动，而从事这种攻击活动的人统一称为攻击者。我们讨论的是他们技术层面的东西：如何攻击，至于他们的动机是出于正当的理由，还是不可告人的目的，则不是我们这里要讨论的内容。

本教材的目的，主要是从计算机学科的角度出发，结合其他的学科，说明网络安全中存在的主要问题以及相对应的解决方法。探讨如何通过综合采用技术手段和管理手段，增强个人计算机系统以及网络的安全性。在此基础上，如何建立网络中的信任，防止网络诈骗，保证网络交易的合法性，并防止信息泄露。

本教材是在读者对计算机学科有一定的了解基础上编写的，如程序设计、操作系统、网络原理及应用、汇编语言等学科。

## 1.2　网络安全威胁

网络的互联拓展了计算机应用的空间，但互联技术本身以及计算机系统存在的弱点，也使得所有网络用户因为彼此互联而更容易被攻击。因为我们通过网络，和现实社会中形形色色的人联结到了一起。

如图 1.1 所示，A 和 B 是网络中的两个用户，C 是联接在网络上的第三方，A 和 B 之间进行通信，面临的主要问题包括 C 对 A 或 B 非授权的访问、C 冒用 A 或者 B 的身份、C 使 A 或 B 无法使用网络等。

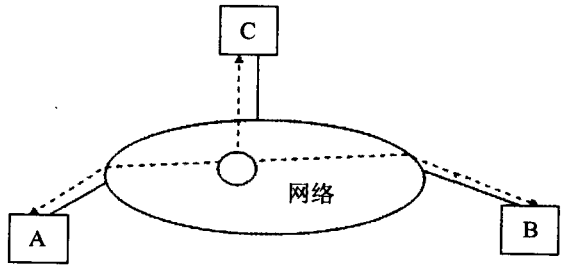



**图 1.1　典型网络连接及安全问题**

因此，归结起来，网络中的安全风险主要有以下几种：

**1. 保密性(Confidentiality)**

通信双方的信息内容有可能被第三方获得。

例如图 1.1 中，当 A 和 B 通信时，在不安全的网络环境中，其通信内容可能被第三方 C 截取。

以下是几种典型的情况：

(1) 电磁辐射的监听

数据信号的传输通常通是过一定频率的电信号在金属导体或者无线的环境下传输，或者是通过光脉冲在光纤中传输。而对于前者，总会产生一定的电磁辐射，通过灵敏的仪器获取、分析这些电磁辐射，就可以了解传输的内容。

(2) 电话线路中的搭线窃听

这也是较古老的信息获取方法，在电话线上搭接一根线和一部电话机，就可以知道这根线上通话的内容。如果将电话机换成一个协议分析设备，就可以对传输的信息进行分析、窃听。

(3) 共享网络中的信息监听

对于共享以太网、无线网络等，任意一台连接到网络中的计算机，都可以通过运行数据包监听程序(sniffer)，捕获数据进行分析。

(4) 其他方式

光纤通信虽然不会产生电磁辐射，但攻击者如果可以物理接触到光纤，则也可以通过如分光器之类的设备监听数据。

攻击者可以利用一些伪装技术，设法获得用户的流量并加以分析。

攻击者如果设法控制了重要的网络设备，如路由器、交换机等，则可以很容易得到各种用户流量，进行分析。当然，这种攻击的难度比较大。

为了保护通信的机密信息内容，防止第三方获取，发送方需要对信息进行加密，而接收方则要进行解密。

### 2. 认证(Authentication)

认证即通信的双方需要确认彼此是要通信的对象，而非假冒伪造的通信方。

当人和人面对面说话时，我们很清楚要通信的对方是谁——通过识别对方的面孔；当打电话时，也基本可以知道说话的对象——通过识别对方的声音。但是，当通信的双方无法“看”到或“听”到对方时，如何保证通信的对方不是假冒的就成了一个问题。

例如，当你收到一封电子邮件，里面声称是你多年未见的老同学，你是否就相信呢？或者你收到一个银行的邮件，声称为了系统维护或其他原因，要求你说出自己的帐号等信息，你是否就会那么做呢？即使收到的信件是来自自己的熟人，但信的内容是否真是他本人所写呢？

在图 1.1 的例子中，如果 A 机器只允许 B 机器访问自己，该如何确认 B 的身份呢？如果 C 模仿成 B 与 A 通信，又该如何识别？是通过 IP 地址、用户名和口令还是其他信息？

这些问题，都是需要通过认证来解决的。

### 3. 完整性(Integrity)

完整性即信息在传输的过程中无法被篡改，或者即使被篡改了，也可以被发现。

现实生活中，经常有这样的情况：甲可能会要求乙给丙捎个话，但当丙听到这些话时，无法确定这就是甲的原话。乙可能出于主观原因(讨厌甲或丙)，篡改原话的内容；乙也有可能因为记忆不好，漏了某些内容。

同样，在数据通信过程中，信息不仅可能被监听，还有可能被修改。例如，即使 A 和 B 之间的通信是保密的，C 无法了解其内容，但 C 仍然可以破坏他们之间通信的内容。

因此，不仅通信的双方要彼此认证，通信的内容的完整性也需要保证。

### 4. 不可否认性(Non-repudiation)

在电子交易过程中，发出信息的一方无法否认其行为也是非常重要的。例如，甲的话引起了某些纠纷的时候，甲会否认自己曾经说过这样的话，但如果有录音，甲就无法否认。或者甲欠了乙 3 000 元，如果乙有甲的欠条，就可以在甲赖帐的时候寻求法律解决的方式。

在电子商务中，如果 A 向 B 发出了一个定单，或者 A 收到了 B 的一笔款项，如何保证 A 无法否认做过这样的行为？

因此，信息的不可否认性是也是一个安全问题，尤其是在电子商务中更为重要。

### 5. 可用性(Availability)

可用性是指网络基础设施、硬件系统、软件系统等在任何时候都是可靠运行，且能被

用户正常使用的。由于网络的作用越来越重要，所以人们会用网络来做更多的事情，如一个公司可以连接他们的客户、供货商、合作伙伴、内部工作人员，进行招聘、广告、收发信件、发布消息、签定合同、购买商品等。

对于这类公司，只要几个小时不能使用网络，业务就会受到很大的影响。有些公司，如 Amazon，是完全靠网络来完成其业务的，因此，其网站的可用性直接关系到公司的生存。

网络上连接的任意一台计算机都具有两种角色：服务的提供者和服务的使用者。当一台计算机通过网络对外提供服务时，同时自己也处于被攻击的风险之中；同样，当一台计算机通过网络使用外面的服务时，也处于被攻击的风险之中。攻击的后果可能是系统被破坏，或者提供的服务不可用。

主要的网络攻击或者相关的活动如下：

(1) 扫描(Scan)

通过向目标(网络、主机等)发一些特定的数据包，并分析响应的结果，了解目标的有关特征，为进一步的攻击做准备。

(2) 入侵(Intrusion)

利用不同的方法，如口令猜测、漏洞攻击等，进入到被攻击的系统上，对其资源进行非授权访问。

(3) 拒绝服务(Denial of Service)

通过产生大量的无用数据包，使得网络、主机或者应用无法被合法的用户所使用。

(4) 滥用(Misuse)

例如散布垃圾邮件、有害信息等。

这些活动都有可能导致系统的不可用，或者非授权的访问。

要解决上述这些安全问题，需要综合运用多种技术手段和管理手段。其中，保密性、认证、完整性、不可否认性等问题，主要基于密码算法及其应用。而可用性涉及到更多的因素，如访问控制、管理等。因此，我们将在介绍有关攻击的基础上，介绍加密技术及其应用，以及各种常见安全防护手段。说明如何发挥人的作用，通过有效的安全管理，综合各种技术手段，从而达到比较安全的防护效果。

另外，从信息系统面临的威胁来看，最具破坏性的主要来自内部。在内部威胁中，危害性最大的就是内部关键人员为了某种利益从事的攻击、破坏活动。对工作不满、遭到辞退、或者与外部勾结的工作人员，往往更容易获取和破坏内部的关键信息。工作中的漫不经心，也经常会导致各种漏洞。

因此，如果发现了一个攻击者声势很大地对系统进行入侵、破坏，实际上产生的危害并不算大。因为那很可能是一个业余攻击者，使用从网络上获得的攻击工具“练手”。危害最大的是那些不动声色的“专业”攻击者，他们可以长期地对信息进行窃取、修改，并使自己攻击的活动很隐蔽，不被发现。

综上所述，我们可以对网络安全防护的定义如下：

拒绝未经授权的物理或电子入侵、操作，保证网络和所传信息端到端的完整性，能够抗拒各种类型的破坏，包括电子袭击、物理袭击、人为错误等。

## 1.3 网络安全的困难性

网络安全问题虽然出现的时间不长，但看起来似乎和现实安全问题一样，将会是一个永恒的问题，短期内不会有一个好的解决方法。和现实安全一样，网络安全也是一个很困难的问题，我们可以从以下几个方面来说明其困难性：

### 1. 攻击与防守的不对称性

网络中的攻击者通常不遵循网络默认的一些规则，利用软件或者协议上的漏洞，或者通过贿赂、勾结内部人员等达到攻击目的。

如果我们观察一个攻击者，可以发现其攻击是有备而来的，攻击工具较容易获得，攻击风险低、难追踪。对于防卫人员来说，则意味着必须要堵住所有可能的漏洞。这如同大江的堤坝，在洪水到来的时候，任何地方都不能疏忽，一个地方有漏洞，整个堤防就可能毁于一旦。Internet 不断增加的复杂性、协议与应用的不断增多等都使得安全防护的难度加大。

我们也可以把安全问题看成是一条链，最脆弱的一环可以使整个系统崩溃。例如，Netscape 的安全性因为其随机数发生器的漏洞，使得整个安全设计都变得不安全。从这个角度来看，100%的网络安全是非常难做到的。

因此，攻击和防守是很不对称的。

### 2. 安全的动态性

尽管我们可以采取许多技术来进行安全防范，但随着时间的推移，操作系统、硬件平台、应用软件、网络协议等都会发生变化。例如，采用了新的服务器，系统升级，出现了新的协议，开发部署了新的应用等。在这个过程中，原来存在的一系列安全问题，如操作系统漏洞可能不存在或者不重要了，但新的漏洞可能又出现。因此，为了应付新的安全风险，网络安全防范也永远处于动态之中，不可能存在什么一劳永逸的技术或解决方案。

网络安全如同军备竞赛，但不同的是，攻击者总是占有优势。防卫者必须要防止每个漏洞，而攻击者只需要找到一个漏洞。攻击者是有专业知识和经验的，而大部分用户却只会使用。

“道高一尺，魔高一丈”用在这里是再恰当不过的。

### 3. 投入和产出问题

在网络安全方面，投入和产出的含义很广，既可能是资金、人力，也可能是时间、易用性。

例如，网络安全在很大程度上是一个投资的问题。为了让信息系统更安全，可能需要使用很多安全设备和技术，雇用许多安全专业人员。所以，拥有的计算资源越多，就越可能达到更好的安全程度。

但这里就有一个矛盾：假设要保护的资产价值为 M，而安全投入为 m，如果 m>M，或者 m 接近 M，则安全投入就失去了意义。同样，这个矛盾对于攻击者也存在，攻击的代

价如果超过了攻击的获益，也是没有意义的。

另外，信息服务的本质是开放性的，或者是部分开放，或者是完全开放。例如，提供检索的搜索引擎、新闻网站、各种公共信息网站是面向所有用户的；企业信息是针对部分对象，如企业与企业之间、企业对用户、企业对内部职员等。而采取各种网络防范措施就意味着限制这种开放性，必然给使用带来不便。

有时候，安全的攻防就像是互相“斗富”，谁拥有的资源(计算能力、专业人员等)更多，谁就更有可能占上风。但安全措施不一定越多就越好，如果大家到银行的柜台前都要经过各种烦琐的安全检查，则银行的业务一定会受到影响。因此，以合理的代价达到一定程度的安全更为现实可行。

从这个意义上来讲，各种网络安全技术及措施是一种均衡。其目的是使得攻击的成本加大，增强人们的安全感，而且不至于使系统烦琐得难以使用。

#### 4. 人性的弱点

实际上，不管我们研究出怎样的安全防护技术，可能最终会发现，安全问题的根源在于人性的弱点，不论是攻击者还是防卫者，都是如此。

攻击者的动机包括好奇心、出名、获取利益、发泄、政治或军事原因等，这些动机和导致社会问题的动机是一样的。例如，如果一个房间的门或者窗户总是紧闭的，周围的人总想要知道，里面到底有什么东西？

而对于防卫者来说，弱点则是麻痹和懒惰。每当一场危机来临的时候，如洪水、瘟疫发生时，人们的安全意识会很快上升，甚至会达到风声鹤唳，草木皆兵的程度。遗憾的是，危机一过，人们很快就会恢复到常态，直到下次危机才被唤醒。

网络安全也一样，人们总是认为自己不会成为攻击者的目标，或者总是认为有网络安全管理人员、网络专家来料理一切。由于这种弱点，以及没有安全经验的用户不断出现，使得网络中的脆弱点总是存在的。同时，网络中存在的“互联”、“信任”，可能使任何一个普通用户都可能通过这种信任链到达一个重要的目标。

可以预料，只要人性的弱点存在，不管安全技术如何发展，安全问题总是存在的。这样看来，是永远没有 100%的网络安全了，既然如此，我们为什么还要讨论网络安全技术呢？现实社会中虽然有假钞，信用卡也会被偷窃，但人们仍然在大量使用，因为其带来的方便程度超过了可能的损失。人们会在家里安装防盗门，保险柜等，虽然不能万无一失，但大部分情况下仍能起作用，并给人们带来安全感。

因此，通过网络安全技术和管理手段，最大限度地减少风险，增加攻击者的成本，给用户带来安全感，并使正常的交往、业务能够进行下去，就是网络安全防护的目标。

多年以来，网络安全更多地被作为一个技术问题来研究，关注的焦点也始终是技术，如加密技术、安全访问控制技术、安全监控技术等。但决定战争胜利的决定因素是人，而不是武器，只有用先进武器武装起来的高素质人员，才最具有战斗力。同样，具有安全专业知识的人员，并辅助以一定的技术手段，才是最有效的防护。

本教材虽然也介绍各种网络安全技术，但贯穿始终的一种思想是：

不管这种技术看起来是多么的完善，必须要有人的参与，配合以良好的安全管理措施，才能够较好的发挥作用。因此，建立安全意识，强化安全管理更为重要。

## 1.4 网络安全组织与机构

目前有许多组织机构开展网络安全方面的研究和应用，本书也引用了很多出自这些机构的各种材料。因此，有必要对这些机构做一个大致的介绍。

1. IETF(www.ietf.org)

本教材的许多内容，都涉及到了 IETF 的相关工作。

IETF(Internet 工程小组)是一个大型、开放的国际组织，由网络设计、运行、研究、厂商等方面的人员组成，共同推动 Internet 体系结构和运行的发展。该组织的开放性是 Internet 成功的主要原因之一。

Internet 各项标准都通过 IETF 制定，IETF 的标准、草案等通过 RFC 文件来发布，并按顺序编号，RFC 越新，编号就越高。关于 RFC 格式、提交过程的详细说明，可以参看 RFC 2026。每个成员都可以提出建议，发布在网络上，供其他人讨论、反馈，最后形成草案和标准。

IETF 是民间性质的，在 Internet 发展初期，IETF 花了许多力量来解决网络的互联互通问题，而安全问题很少涉及。读者如果翻看 IETF 早期的文档，就会注意到这一点。当 Internet 发展到商业化的规模后，安全问题日益突出，IETF 也把许多注意力放在了网络安全上。对于 Internet 的许多传统协议，如 IP、TCP、TELNET、FTP、DNS 等，IETF 都提出了新的安全增强或者改进协议，如 IPsec、TLS、SSH、DNSSEC 等。同时，对于“防火墙”、IDS、PKI、认证等技术的应用，IETF 也提出了许多新的 RFC，有的已经成为了标准，有的仍然在讨论之中。

IETF 专门成立了一个安全工作小组，其中又分了 19 个小组，研究各种网络安全技术及在 Internet 中的应用，如安全邮件、网络层安全、PKI、认证技术等，各个小组的职能如表 1.1 所示。

表 1.1 IETF 安全工作小组

| 工作小组 | 职 能 |
| --- | --- |
| aft | “防火墙”认证 |
| cat | 通用认证技术 |
| idwg | 入侵检测事件交换格式 |
| ipsec | IP 安全协议 |
| ipsp | IP 安全策略 |
| ipsra | IP 安全远程访问策略 |
| kink | 基于 Kerberos 的网络密钥协商 |
| krb-wg | Kerberos 工作组 |
| msec | 组播安全 |
| openpgp | 安全电子邮件 PGP 标准 |