青松®

网络安全与黑客

新时代工作室□编著

青岛出版社

网络安全与黑客

新时代工作室　编著

青岛出版社

鲁新登字 08 号

内 容 简 介

“没有黑客，网络不安全；有了黑客，网络更不安全”。黑客的攻击总是与网络的安全性紧密相关，正所谓道高一尺、魔高一丈。本书全面深入地分析了网络安全与黑客间较量、发展的规律和实质。书中也深入细致地讲述了如何防止入侵，如何用其人之道，还治其人之身。

系统和网络所面临的安全威胁并不是固定不变的，新问题不断出现，而且没有绝对消失的一天。本书介绍这些的目的在于，使您对安全问题的规律和实质有一定的认识，在面对新的问题时，不会因为出乎意料而措手不及。

本书既适合负责网络安全的专业人员来学习，也适合一般的电脑用户阅读。

图书在版编目(CIP)数据

网络安全与黑客/新时代工作室编著. - 青岛：青岛出版社，2000.4
ISBN 7－5436－2254－1
Ⅰ. 网…
Ⅱ. 新…
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（2000）第 16951 号

书　　名	网络安全与黑客
编 著 者	新时代工作室
出版发行	青岛出版社
社　　址	青岛市徐州路 77 号(266071)
邮购电话	(0532)5835124　5814750　5835844
责任编辑	樊建修　金利鹏
装帧设计	申　尧
印　　刷	胶州市装潢印刷厂
出版日期	2000 年 7 月第 1 版，2000 年 7 月第 1 次印刷
开　　本	16 开(787×1092 毫米)
印　　张	13.75
字　　数	330 千
印　　数	1－3000
ISBN	7－5436－2154－1/TP・273
定　　价	26.00 元

出版者的话

有史以来，没有哪一门科学能像电脑这样飞速发展！新技术层出不穷，新产品不断涌现，电脑工作者必须不断学习、更新知识，才能跟上形势，不被淘汰。然而人们的精力是有限的，面对良莠不齐、铺天盖地而来的各种电脑著述和技术资料，你不可能有很多的时间一一鉴别和阅读。这时就需要专家们根据自己的实践经验给以精选和引导。

为此，青岛出版社聘请了具有丰富教学经验和实践经验的专家，组成《青岛松岗电脑图书》编委会，向广大读者介绍适合我国国情的、最新最实用的电脑及网络技术。

《青岛松岗电脑图书》编委会对这套丛书的质量负责，并郑重承诺：编、校、印刷质量符合国家新闻出版署的质量要求——差错率低于万分之一。

《青岛松岗电脑图书》编委会由以下人员组成：

目 录

第 1 章　黑客及其表现

1.1　有关黑客的一些概念

1.1.1　什么是黑客

“黑客”是英文“Hacker”的译音，是一个充满神秘气息的称谓，原意为热衷于电脑程序设计的人。但这些人不同于普通的电脑迷，他们把掌握的高科技专门用来窥视别人在网络上的秘密。比较典型的黑客是一些拥有计算机和调制解调器的青少年。他们以攻入计算机系统为挑战，并以此证明自己的能力。他们通过 BBS 与朋友通信，并交流他们发现的一些计算机系统的用户名、口令和其他信息。

最早的黑客大概要从入侵电话系统开始算起，黑客用 ratshack 拨号器(一种被称为红箱子的东西，它是用于传输数字声音的手提式电子设备电话)，编程模拟硬币投入付费电话的声音。这样，他们就能在大多数的收费电话亭免费打电话了。

一般说来，作为黑客，他们也有自己的一些守则，当然这也是人们所希望的。如果每个黑客都遵守这些守则，那我们就不用担心自己的计算机系统遭到这样或那样的恶意攻击了。

1.1.2　常见的黑客入侵方式

(1) 口令入侵

所谓口令入侵就是指用一些软件解开经过加密的口令文件，但是许多精于此术的黑客并不采用这种方法，而是用一种可以绕开或屏蔽口令保护的程序。对于那些可以解开或屏蔽口令保护的程序通常被称为 CRACK。由于这些软件的广为流传使得入侵电脑变得很简单，一般不需要很深入的了解系统的内部结构。此内容将在后面作更详细的说明。

(2) 特洛伊术

说到特洛伊，只要知道这个故事的人就不难理解，它最为广泛的方法是把一个能帮助黑客完成某一特定动作的程序依附在某一合法用户的正常程序中，而一旦用户触发该程序，那么依附在内的黑客指令代码同时被激活，这些代码往往能完成黑客指定的任务。由于这种入侵法需要黑客有很好的编程经验，且要更改代码、要一定的权限，所以较难掌握。也正因为它的复杂性，一般的管理员很难发现。

(3) 监听

这是一个很实用但风险也很大的方法，但是还是有很多的记录显示入侵采用了此类方法，正所谓艺高人胆大。网络节点或工作站之间的交流是通过信息流的转送，而当在一个没有集线器的网络中，数据的传输并没有指明特定的方向，这时每一个网络节点或工作站都是一个接口。在这样的“接口”上，用一个叫 sniffer(软，硬都有)的装置，截获口令这类秘密的信息，就可以用来攻击相邻的网络。

另外还有 Email 技术、病毒技术和隐藏技术。

以上只是入侵方法中的很小一部分，在世界各地的黑客们以飞快的速度创造着新的入侵方法。

1.2 黑客的攻击行为

为了让读者对黑客的行为有一个大体的认识，更好地防止自己的计算机免受黑客入侵，这一节简略地介绍黑客常有的攻击行为。

1.2.1 攻击的目的

对攻击者的目的有一定了解，可使我们更好地对付可能的攻击。下面我们介绍黑客们一般想要达到的目的。

(1) 控制中间站点

黑客在攻击得手后会做些什么，是个许多人关心的问题。一些攻击者在登上目标主机之后，只是运行了一些程序，这些程序可能是无害的，仅仅是消耗了一些系统的处理器时间。在一些情况下，攻击者为了攻击一台主机，往往需要一个中间站点，以免暴露自己的真实所在。即使被发现了，也只能找到中间站点的地址，与己无关。在另一些情况下，假使有一个站点能够访问另一个严格受控的站点或者网络。例如，能够连通到另一个主干网上去，攻击者为了访问另一个主干网的一些站点，往往把这个站点当作中间站点，就需要先攻击这个中间站点。

这种情况对作为中间站点的目标主机本身并无多大坏处，但是潜在的危害已经存在。首先，它占用了处理器时间，当运行一个网络监听软件时，会占用大量的处理器时间，将使主机的响应时间非常长。另一个可能的危害是，这种行为将一种责任转嫁到目标主机的管理员身上，后果是难以估计的。还有可能将一笔账单转嫁到受害者一方。

(2) 获取口令

攻击者的目标是系统中的重要数据。因此攻击者通过登上目标主机，或者使用网络监听程序进行攻击。监听到的信息可能含有非常重要的信息，比如是用户口令文件。口令是一个非常重要的数据，当攻击者得到口令，便可以顺利地登录到别的主机，或者去访问一些受到限制的资源。

一般情况下，一个攻击者入侵之后，他都会翻看当前用户主目录下的文件，复制系统的/etc/hosts 或/etc/passwd 文件。

(3) 获得超级用户权限

如果具有超级用户权限，就可以做任何事情，所以每一个入侵者都希望能得到超级用户权限。取得这种权限，便可以完全隐藏自己的行踪；可在系统中埋伏下一个方便的后门；可以修改资源配置，为自己得到更多的好处等。

在 Unix 系统中，运行网络监听程序必须要有这种权限，因此在一个局域网中，如果掌握了一台主机的超级用户权限，可以说就掌握了整个子网。

(4) 对系统的非法访问

有许多系统是不允许其他用户访问的，必须以一种非常的行为来得到访问权力。

这种攻击的目的并不一定是要做什么，只是为了访问而攻击。在一个有许多 Windows 95 系统的网络中，常常有许多用户将自己的目录共享出来，若攻击者得手后他就可以从容地在这些计算机中浏览、寻找自己感兴趣的东西，或者删除、更换文件等。

(5) 进行不许可的操作

在一个 Unix 系统中，没有超级用户权限，许多事情便无法去做，于是很多用户在有了一个普通的户头之后，总想得到更大一点的权利。

许多用户都会有意或无意地去尝试尽量获得超出允许的一些权限，于是便寻找管理员在设置中的漏洞，或者去寻找一些工具来突破系统安全防线。例如，特洛伊木马便是一种使用很多的手段。

(6) 拒绝服务

同上述目的相比较，拒绝服务便是一种有目的的破坏行为了。拒绝服务方式的攻击很多。在后面的专门介绍拒绝服务方式攻击的章节中将有详细的论述。

(7) 窃取信息

窃取信息包括涂改信息和暴露信息。

涂改信息包括对重要文件的修改、更换、删除。这是一种很恶劣的攻击行为，不真实或者错误的信息往往会给用户造成很大的损失。

入侵的站点往往有许多重要的信息与数据可用。如果把这些信息直接发往自己的站点也会暴露自己的身份和地址。于是窃取信息后，黑客往往将这些信息和数据送到一个公开的 FTP 站点，或者用电子邮件寄往一个可以拿到的地方，等以后再从这些地方取走。这样做可以很好地隐藏自己。

将盗取的重要信息发往公开的站点会造成信息的扩散，因为那些公开的站点常常会有许多人访问，其他的用户完全有可能得到这些信息，并再次扩散出去。

1.2.2 实施攻击的人员

(1) 计算机黑客

比较典型的黑客是一些以攻入计算机系统为挑战，并证明自己的技术的有计算机和调制解调器的人。

(2) 不满或者被解雇的雇员

虽然只有少数不满或者被解雇的雇员会对系统进行攻击，他们做这些通常是会比较顺利，因为他们非常了解网络的安全状况。

这类人知道许多调制解调器的号码和系统中的一些后门。他们可能破坏 Web 服务器或使之无法正常工作。而且他们对服务器、小应用程序以及脚本程序非常熟悉，并且也知道系统的脆弱性。

因此程序管理员应定期更换密码，定期删改账号，以减少这种威胁。

(3) 极端危险的罪犯和工业间谍

在职员工和黑客也可能取得专用数据，并提供给别的公司或组织而获得利益，成为工业间谍。当前工业间谍正呈上升趋势，所盗取的重要信息包括生产和产品开发信息；销售和价格数据；客户名单以及研究和计划信息。

有些间谍是政府或者组织雇来专门窃取秘密数据的人；有时也是指组织中使用计算机的员工，为个人的发展在计算机上寻找数据。

1.2.3 常见的工具

了解黑客常用的入侵工具，我们可以判断自己的计算机遭到攻击时会有哪些表现，是受到了哪种入侵，从而有的放矢地进行防御。除非攻击者自己开发工具，否则它必须利用现成的工具。

黑客经常利用一些别人使用过的并在安全领域广为人知的技术和工具。尽管许多工具找到的系统漏洞早已不是秘密，但是，许多系统中这些漏洞仍然存在，并没有得到系统管理员的重视。另外，许多管理员对安全关注过少，也是造成入侵和被攻击的重要因素。在一个 Unix 系统中，当入侵完成之后，系统中可能被设置了大大小小的漏洞，完全清理这些漏洞是很困难的，这时候只能重装系统了。当攻击者在网络中进行监听，得到一些用户口令后，只要有一个口令没有改变，那么系统仍然是不安全的，攻击者在任何时候都可以重新访问这个网络。

在 Internet 成千上万的站点上有许多描述系统安全漏洞的文章，还有一些入侵者所作的文章极详尽地描述了这些技术，在这些文章里详细地讲述了如何完成某类攻击，甚至有相应的程序可用。

如果入侵者按这些指导生硬地进行攻击，结果经常令他失望，因为一些攻击方法已经过时了，而且这些攻击会留下攻击者的痕迹。

攻击工具不局限于专用工具，系统常用的网络工具也可以成为攻击的工具。例如，要登上目标主机，

便要用 telnet 与 rolign 等命令对目标主机进行侦察，系统中有许多可以做为侦察的工具，如 finger 和 showmount 。甚至，一些资深的黑客自己可以编写一些工具，这并不是一件很难的事情。

攻击的工具是多种多样的，入侵者将监听程序安装在 Unix 服务器中，对登录进行监听，例如监听 23、21 等端口。一有用户登录，它就将监听到的用户名和口令保存起来，于是黑客就得到了账号和口令。在网上，有大量的监听程序可用。甚至可以自己编写一个监听程序。监听程序可以在 Windows 95 和 Windows NT 中运行。

另外，电脑病毒，如蠕虫病毒也可以成为网络攻击的工具。蠕虫虽然并不修改系统信息，但它极大地延缓了网络的速度，给人们带来了麻烦。

1.2.4 攻击事件

一般情况下攻击的行为比较难界定，也比较难发现。“攻击”通常定义为：攻击仅仅发生在入侵行为完成且入侵者已在目标网络内。但更容易接受的观点是使一个网络受到入侵和破坏的所有行为都应称为“攻击”。也就是说，攻击开始于一个入侵者开始在目标机上“工作”的那个时刻。

入侵者通常需要一段时间来完成攻击行为。就像科技工作者做论文一样，先需要进行一段时间的调研工作。在这段时间，攻击者将收集目标主机的信息，观察目标主机的反应。这些调研工作本身并不能视为攻击，因为它们并未连续发生，并且与通常用户的行为没有什么差别。当入侵者发现目标系统一直在做日志，那他也许会放弃，也许会一直耐心地等待，直到机会出现。

攻击者与安全管理员之间可以说是一场斗智斗勇的较量。攻击者在琢磨着管理员的习惯、技术和水平。同时，系统管理员也要了解攻击者的行为特征，作好防备工作，及时发现异常，堵住系统漏洞。

1.2.5 攻击的三个阶段

(1) 锁定目标，搜集相关信息

选定攻击目标——即准备攻击的系统，以 Unix 系统为例，通常是从已攻入系统的.rhosts 和.netrc 文件所列的主机中挑选，从系统的/etc/hosts 文件中可以得到一个很全的主机列表。但大多数情况下，从中选定攻击目标是一个比较盲目的过程，除非攻击者有明确的目的和动机。攻击者也可能找到 DNS(域名系统)表，通过 DNS 可以知道机器名、Internet 地址、机器类型，甚至还可知道机器的属主和单位。攻击目标还可能是偶然看到的一个调制解调器的号码，或贴在机器旁边的使用者的名字。

(2) 获得初始的访问权与特权

finger 命令不但能测试目标主机是否连通，往往还能告诉攻击者许多有用的信息，例如：

```
$ finger @ target.host
```

于是可以得到类似如下文所示的信息：

[***.***.***.***]

Login	Name	TTY	Idle	When	Where
dsm	Distributed Shared M	console	28	Tue 12:19	
guest	???	pts/0	2:46	Tue 09:28	another.host1
wang1	Wangling	pts/5	14	Tue 11:51	another.host2

注:***.***.***.***为主机 target.host 的 IP 地址

【注意】finger 是攻击者很有用且很常用的命令，它可以监视目标主机上用户的情况，因此最好将这项服务关闭。在 Unix 系统中，还有一些这样的服务。

而口令就不容易获得了，特别是用户口令通常为 8 个字符，又不是字典中的词，其组合有非常多的可能性。攻击者若使用口令获取工具，也相当费时且不能保证奏效，至少它需要足够的耐心和时间。而且对于 Windows NT 和一些主要操作系统来讲，系统在三、五次试口令仍然失败的情况下会断掉连接。这就是为什么攻击者总是依赖网络服务，如 NIS、RLOGIN/RSH 与 NFS 等攻击系统的原因。

在一些系统中，可以配置为三次输入口令不正确，就将该用户账号锁住，使其不能再登录。这就有效地保护了系统的安全。但这也可能造成一个拒绝服务的攻击，因为在系统管理员解锁之前，合法的用户也进不去了。

当系统存在设置漏洞或者系统本身并不是安全时，获得特权不是没有可能的。甚至可以小心的构造一个特洛伊木马程序让用户上当。但是这种方法慢，而且不一定奏效。

现在，在许多软件中发现了一类称为缓冲区溢出的错误。在 Unix 系统中，利用一些 SUID root 程序的这种错误编写的程序可以帮助攻击者轻易地获得系统特权。

(3) 攻击其他系统

攻击一个系统得手后，攻击者往往不会就此罢手。他会在系统中寻找相关主机的可用信息，继续进行攻击。

1.2.6　常见的攻击时间

让读者了解了黑客一般在什么时候进行攻击，可以使他们在最危险的时候提高警惕，防止遭到攻击。

在 Internet 网络上的攻击是不确定的。因为绝大多数网络都是 24 小时不间断地和 Internet 相连，这意味着攻击可以发生在任何时间。通常，攻击的行为可能会有下面的一些规律。

就每天看来，大部分的攻击(或至少是商业攻击)时间是服务器所在地的深夜。人们也许认为攻击者会在白天(目标所在地的时间)发生攻击，因为大量的数据传输和交换能掩盖他们的行为。有以下几个原因可以说明为什么攻击者避免在白天进行攻击：

① 客观原因，在白天大多数攻击者要工作、上学或在其他环境中花费时间，以至没有时间进行攻击。也就是说他们不能整天坐在计算机前面。

② 网络正变得越来越拥挤，因此最佳的工作时间是在网络能提供高传输速率的时间。最佳的时间段会根据目标主机所在地的不同而不同。身在美国西南部的某人最好在伦敦当地时间晚上 10 点到凌晨 6 点之间进行攻击，因为晚上这段时间以前会遇上伦敦当地的网络使用高峰(当地人正检查他们的邮件，用户正浏览最新新闻等)。

③ 为了躲避网络管理员。假定在某时某入侵者发现了一个漏洞，如果此时有管理员在工作，入侵者能有何举动？恐怕很少。正在工作的系统管理员一旦发现有异常现象(例如它使用了 netstat 或者 ps 命令)，很容易发现入侵者的踪迹，他便会跟踪而来。另外，在冬季的攻击比夏季频繁。

1.3　本章小结

本章主要介绍了有关黑客的一些基本情况。Internet 是一个奇妙的世界，因此能够吸引大量的具有好奇心与挑战精神的人希望深入到它的内部，而其中不可避免的存在一批拥有强大破坏欲的人，这些人被笼统地定义为黑客。不管他们的动机有没有危害性，他们对网络都有很深的了解。

本章还对当前网络攻击的目的、人员、时间以及工具等进行了分析。介绍这些的目的在于使你了解其规律和实质，因为系统和网络面临的安全威胁并不是固定不变的，旧的漏洞被更正，同时新的问题又源源不断地被发现，没有绝对消失的一天。但是，当我们对系统和网络安全问题的规律和实质有了一定的认识之后，面对新的问题时，才不会因为出乎意料而措手不及，才能应付自如。

第 2 章　网络安全及其面临的挑战

2.1　网络安全的定义

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续可靠正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

网络安全的具体含义会随着“角度”的变化而变化。一般的网络安全指的是网络系统或者主机终端的数据保密安全和用户权限的分层限制不受侵犯。

网络安全应具有以下四个方面的特性：

① 保密性：信息不泄露给非授权用户、实体供其利用的特性。

② 完整性：数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

③ 可用性：可被授权实体访问并按需求使用的特性。即当需要时能否存取所需的信息。例如网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

④ 可控性：对信息的传播及内容具有控制能力。

2.1.1　物理安全

物理安全指用以保护计算机硬件和存储介质的装置和工作程序。由于计算机和其他物理物体之间的相似之处，因此物理安全是计算机安全的最重要的方面，这是最好理解的。

像打字机和家具一样，计算机也是偷窃者的目标，一张软盘完全可以装在口袋里带走。但是不同于打字机和家具，计算机偷窃行为所造成的损失可能远远超过计算机本身的价值。因此必须采取严格的防范措施，以确保计算机设备不会丢失。

实际上目前有许多确保安全的设备。比如在计算机下面安装将计算机固定在桌子上的安全托盘，用高强度电缆在计算机的机箱中穿过等。还有就是要加强计算机机房的管理，如门卫；出入者身份检查；下班锁门以及实施各种硬件安全手段等预防措施。

物理安全还包括防止损害计算机，如不要将咖啡溅在磁盘上，不要猛力震动硬盘等。

备份(Backups)也是保证安全的一项重要措施。

“备份”的意思是指在另一个地方制作一份拷贝。这个拷贝或备份将保留在一个安全的地方，一旦失去原件，就能使用备份。应该有规律地备份以便使用户避免由于硬件故障导致的数据损失。

备份对防卫人为破坏(human subverter)也至关重要。如果计算机被偷，数据的惟一的拷贝还在备份上，这是可以在另一台计算机上恢复的。如果计算机黑客攻破计算机系统里并抹掉所有文件，备份将能把它们恢复，假定这个计算机黑客确实无法获得备份或者知道备份的存在。

但是，备份也是潜在安全问题。间谍把它当成偷窃的目标，因为备份含有秘密信息的精确拷贝。确实，备份给计算机系统提供更大安全性，因为偷窃含有工作数据的介质比偷窃备份更引人注目。

由于备份存在安全漏洞，一些计算机系统允许用户的特别文件不进行系统备份。这样的行动是因为备份磁带被偷的损失比由于设备故障失去数据的损失更大。

2.1.2　逻辑安全

计算机的逻辑安全需要用口令字，文件许可，查账等方法来实现。防止计算机黑客的入侵主要依赖计算机的逻辑安全。

高度机密的信息是完全的与其他各种数据相隔离，对所有高度机密的数据的存取都被严格地控制着。计算机安全的一个重要问题是：我们试图保护的信息——电子信息，其本身有特殊性质：当有人窃走我们的信息时，他并不需要将信息从计算机文件中移走。

我们可以使用软件来保护存于计算机文件中的信息，该软件限制了其他人存取非自己所有的文件，直到该文件的所有者明确准许其他人可以存取该文件时为止。限制存取的另一种方式是通过硬件完成，在接收到存取要求后，先询问并校核口令，然后访问列于目录中的授权用户标志号。此外，有一些安全软件包也可以跟踪可疑的、未授权的存取企图，例如，多次试登录或请求别人的文件。显然，我们可以限制试登录的次数或对试探操作加上时间限制，在此之后，系统就自动地退出。现有的各种技术提供了高水平的计算机安全，特别是计算机上的军事安全保密，想要破坏大多数含有保密信息的计算机的安全控制，其代价是非常昂贵的。当然维护这样高级的安全的代价通常是将各计算机隔离，以及使进入计算机的手续操作麻烦。但随着安全技术的进一步提高，将会大大有助于减低这种代价，使整个安全控制对合法用户更透明一些。因为随着新一代计算机的研制也发展了“用户友好”界面，故在发展和加强计算机的安全系统时，也充分注意到了用户的相同需要。

2.1.3　操作系统提供的安全

在计算机中能够控制基本操作的程序，即操作系统。操作系统是计算机中最基本、最重要的软件。同一计算机可以安装几种不同的操作系统。例如，PC 机可以运行 MS-DOS 操作系统，也可以运行 Windows 操作系统。PC 机在这两种操作系统下，具有完全不同的状态。

如果计算机系统可提供给许多人使用，操作系统必须能区分用户，以便于防止他们互相干扰。例如，多数的多用户操作系统，不会允许一个用户删除属于另一个用户的文件，除非第二个用户明确地给予允许。

一些安全性较高、功能较强的操作系统可以为计算机的每一位用户分配账户。通常，一个用户一个账户。操作系统不允许一个用户修改由另一个账户产生的数据。账户名通常由一到八个字母或者数字组成，典型的用户名，如“simsong”，“Garfinkel”，“slg”，“SIMSON”或“ML1744”。

多数的操作系统需要一个用户拥有账户名(account)和密码(password)以便使用账户。账户名字一般是公开的，口令是秘密的，只有这个用户和操作系统知道。

2.1.4　联网安全

联网的安全性只能通过以下两方面的安全服务来达到：

① 访问控制服务：用来保护计算机和联网资源不被非授权使用。

② 通信安全服务：用来认证数据机要性与完整性，以及各通信的可信赖性。例如，基于 Internet 或 WWW 的电子商务就必须依赖并广泛采用通信安全服务。

2.1.5　其他形式的安全

多数的计算机系统的价值是由系统的性能、安全管理所需的时间、实用性和复杂性决定的。许多的政府系统设有专职的“安全管理员”，他们的工作是管理和监控计算机设备的安全运转。许多大学也极为关

心计算机安全，因为他们是计算机黑客的目标。然而，由于缺少经验，多数的商业机构在计算机安全方面非常脆弱。

安全工作又有许多种形式：比如操作系统被设计的能阻止用户读取未授权数据；使操作系统报警和有日志功能；在操作人员接触秘密数据前，进行全面的安全教育。最后也许是物理安全形式，如安装锁和报警系统以防设备和存储介质失窃。

在安全的环境中，许多类型的安全工作是互相加强的，并如果一道安全防线失败，另一道安全防线将防止入侵或者最大限度地减少损失。

2.1.6 虚假安全

虚假的安全靠得是别人知道甚少和安定。虚假的安全不是安全的一种形式，虽然经常被错认为是安全的。原因之一是没有及时通知网站的管理者，某个安全系统被绕过了。或者通常入侵没被侦察到，直到发生了重要损害或者入侵者已变得小心了。等到发现了损害，管理员没有选择，只有安装新的虚假的安全系统，可这个系统并不安全。

有这样一个计算机上的虚假安全的例子。一个小商业者整天使用他的 IBM PC 记录和管理雇员。为了防止雇员发现，他将磁盘上贴上有“DOS 1.0 Backup Disk”的标签。他希望没有雇员在读了这个标签后对磁盘感兴趣。虽然这标签也许的确能起作用，但是有确保这个磁盘安全的更好方法(如在文件橱柜中锁上它)。

虚假安全的典型例子是在门前的垫子下隐藏钥匙。防止窃贼进入这所房子的惟一凭借是——窃贼不知道有一个隐藏的钥匙和它的位置，这样的情况下钥匙的安全是假的。如果进入这所被盗房子的窃贼，把钥匙放回到它的原来的地方，这个家庭将没有人知道这个窃贼是如何进入的。如果这个家庭改变了隐藏钥匙的地点，窃贼需要做的是再找到它。因此，可以说提高安全水平的方法，取决于每一个使用钥匙的家庭成员如何处理钥匙的方法。

另一个虚假安全的例子，是一个秘书用办公室的公用计算机存储她的个人信件。为了隐藏信件她把它们命名为 MEMO1、MEMO2，并且前三页保留了办公备忘录，备忘录后面隐藏她的私人信件。一旦她的秘密被发现，则没有一封信是安全的。

2.2 动态的网络需要动态的安全策略

建立网络的目的在于资源共享和信息交流，但这其中存在安全问题。当您的系统集成商为您精心设计了一个网络信息系统，并采取了一系列安全措施后，如：设置防火墙，采用加密算法进行密钥传输，进行用户身份认证等，您还是觉得有点“玄”。您凭什么认为这样的网络就是“安全的”呢？是根据设计方案文件的厚度？还是为此所花的钱数？到底如何评价一个网络的安全性呢？

曾听说过这样的定义：“网络的安全程度定义为该网络被攻击成功的可能性”。实际上，通常我们总是设法保护装有宝贵信息的机器，然而，网络安全的强度只取决于网络中最弱连接的强弱程度。黑客认识到了这一点，他们寻找网络中未受保护的机器，诸如不常使用的打印机或传真机(为了充分利用这些设备，通常是设置成网络共享的，而且几乎都不需要口令验证)，利用它们跳到具有敏感信息的机器。因此，寻找网络中的薄弱环节和安全漏洞是每个系统管理员和每个黑客都要做的一件事。系统管理员查找漏洞的目的在于加强防护，黑客探测漏洞的目的在于找到攻击点。如果您能测量它，发现它的所在，您才有可能控制它，您才能领先黑客一步。

另一方面，网络是动态的，黑客也是多谋善变的。买安全产品或服务，并仅配置一次是不够的，防火墙如此，其他安全产品也是如此。随着网络中的应用、工作站以及操作系统数量和类型的改变，网络安全的挑战会越来越激烈。黑客会利用不断发现的网络或系统安全漏洞，采用各种新的方式、方法攻击您的系统，因此您的安全策略应该适应它。

在不同环境和应用中的网络安全有不同的内容，如下所述。

① 运行系统的安全，即保证信息处理和传输系统的安全。它侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁泄漏产生信息泄露，干扰他人或受他人干扰。

② 网络上系统信息的安全。包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密。

③ 网络上信息传播的安全，即信息传播后果的安全，包括信息过滤等。它侧重于防止和控制非法、有害的信息进行传播后的后果，避免公用网络上大量自由传输的信息失控。

④ 网络上信息内容的安全。它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。本质是保护用户的利益和隐私。

2.3　网络面临的安全威胁

2.3.1　黑客事件

1993 年底，中科院高能所就发现有黑客侵入现象，某用户的权限被升级为超级权限。当系统管理员跟踪时，被其报复。1994 年，美国一位 14 岁的小孩通过互联网闯入中科院网络中心和清华的主机，并向我方系统管理员提出警告。

1996 年，高能所再次遭到黑客入侵，私自在高能所主机上建立了几十个账户，经追踪发现是国内某拨号上网的用户。

同期，国内某 ISP 发现黑客侵入其主服务器并删改其账号管理文件，造成数百人无法正常使用。

1997 年，中科院网络中心的主页面被黑客用魔鬼图替换。

……

他们或者修改网页进行恶作剧或流言恐吓；或者破坏系统程序或施放病毒使系统陷入瘫痪；或者盗用服务器磁盘空间建立自己的个人主页或站点，传播黄色、反动信息；或者窃取政治、军事、商业秘密；或者进行电子邮件骚扰；或者转移资金账户，窃取金钱。他们对国内的计算机系统和信息网络构成极大的威胁。

正是这些黑客事件的频频发生，尤其是 1999 年 1 月以来国外黑客组织“地下军团”公然对我国各大政府与商业网络的频繁入侵挑衅，信息安全问题越来越多地被提到各级政府和网络管理部门的重要议事日程上来。但人们很快发现，想有效防止黑客的入侵实在不是一件容易的事，即便已经拥有高性能防火墙等安全产品，依然抵挡不住这些黑客对网络和系统的破坏。

黑客通过猜测程序对截获的用户账号和口令进行破译，以便进入系统后做更进一步的操作；或者利用服务器对外提供的某些服务进程的漏洞获取有用信息，深入系统；或者利用网络和系统本身存在的或由于设置错误引起的薄弱环节和安全漏洞实施电子引诱(如安放特洛伊木马)，以获取进一步的有用信息；或者通过系统应用程序的漏洞(如 CGI 程序)获得用户口令侵入系统；当然绕过防火墙进入系统更是他们的拿手好戏。政府、军事、邮电和金融网络是他们攻击的主要目标。尤其是我国的许多网络在建网初期较少或者根本就没有考虑安全防范措施，网络交付使用后，网络系统管理员的管理水平又不能及时跟上，留下了许多安全隐患，给黑客入侵造成许多可乘之机。

2.3.2　计算机病毒

计算机病毒自被发现以来，其种类呈几何级数增长。目前，活体病毒已达 14000 多种，病毒机理和变种不断演变，为监测与消除带来了很大的难度，成为计算机及其网络发展的一个很大危害。