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

们也会将本组织的绝密信息出卖给组织的竞争对手，但这不仅仅是一种蓄意破坏的行为。

1996年在Omego工程公司就有这样一起事件发生。Omega的一名职员Timothy Lloyd发现自己即将被公司开除，于是他在Omega的计算机系统里安装了一个逻辑炸弹程序（一种计算机代码，在一定的时间或特殊的条件下会产生破坏作用）。当Lloyd离开公司后，这种软件有系统有组织地删除了Omega公司所有的合同，更严重的是，Omega公司用于生产过程中独有的专利软件也被删除了。据估计Lloyd所造成的经济损失约有一百万美元，这对于的计算机犯罪所造成的经济损失来说只占一小半，但Omega公司的一名高层人物说，他们永远也无法恢复这次事件所带来的经济损失。由于公司生产能力减少，80名员工被迫失业，Lloyd也于2000年5月受到审判。

已被解雇的员工是根本没有时间实施其报复计划的，但Lloyd在离开公司之前就已经开始进行其报复计划。通常情况下，对于那些即将要被解雇的员工，公司应该撤消他们对计算机系统的访问权。登录口令应该及时修改、访问卡、证件钥匙及手提电脑都应该上交。很少有被解雇的职员会友好地对待工作，那种认为提前两周下达辞退报告但仍希望职员能继续安心工作不受影响的想法是不切实际的。

有种类型的内部入侵者十分普遍，有一个专门的术语来形容他们，《信息安全杂志》2001年第一期中有一篇文章，作者Eric Shaw将他们定义为“Proprietor”。这种人对他的信息技术有极强的独占欲，为了独自占有它们，他愿付诸一切控制这些技术。这些人常常给计算机系统带来巨大的破坏，因为他们在组织里的地位和对信息系统的强大控制力。因此，对于这些人一定要小心提防。

最后一种将会给组织带来威胁的内部人员是那些非正式雇员或短期雇员，但他们在一定限制范围内能访问该组织的计算机系统。股东、顾问等常被发现与全职职员在一块工作。由于要从事某一项具体的工程项目，他们通常获准访问公司的计算机系统，与那些正式的职员一样，他们也有机会避开内部的安全监控，接触到那些他们原本无权访问的信息。

一些大公司经常将安全及监控服务交给别人做。从经济的角度看，这是个很好的做法（他们不用担心维护和人员培训）。但这样会有更多的人有权访问公司的资源，并能经常单独和设备在一起。有的人得到某些监控公司的临时雇佣，就可以访问某公司的信息系统。有些粗心的雇员们下班后忘记注销或把自己的登录口令或用户的访问密码写在抽屉的一张纸片上，这些都为那些企图闯入本公司信息系统的非雇员们提供了可作案的条件。

1.2.2 外部威胁

同内部威胁一样，计算机系统和网络的外部威胁也是形式多样的。

1. 竞争者

首先，最大的危险来自于自己的竞争对手，因为他们往往有强大的经济后盾。竞争者可以是一个公司的商业竞争对手，也可以是攻击另一国的计算机系统的政府情报人员。这些人常常有了某一个具体的目标，要么破坏其计算机系统，要么窃取一些绝密的信息。他们的目标不是公众，因而其攻击行为往往不被人发现，即使被发现也很少被曝光于大众。

我们就拿德国联邦情报局来做例子吧，据FBI的一名代理人Edwin Fraumann的一份报告说，它在德国的Frankfurt城外安装了一个秘密的计算机设备，利用这套设备，它闯入了世界上许多

公司及政府的网络和数据库。但德国官方否认了这一说法。

另一类竞争对手就是获得自己政府支持的外企公司，前国家安全局的雇员 Iva Winkler曾在书中写到，某些国家为了从事针对某国尤其是美国的情报活动，在那些国家里投资建立了公司。《Corporate Espionage》一书中，Winkler谴责俄罗斯、伊朗、古巴参与了这种针对美国公司的情报活动。所列举的国家中还包括一些历来与美国联盟的国家，如日本、法国、以色列和德国。

2. Hacker、Cracker和Phreaker

最为公众熟知的外部攻击者，就是媒体所指的 hacker、cracker和phreaker。然而并非所有的人都认同对这些术语的解释，因特网上的一个文件《 Hacker Jargon File》做出了对这些术语最能让人接受的定义。根据这个文件，对 hacker的解释是：

1) 他们喜欢探究那些程序化的计算机系统的细节，喜欢施展自己的才能，而大部分用户只懂得一点点必要的计算机知识。

2) 他们着迷于甚至疯狂地编程，或者说他们喜欢编程胜过于建立关于编程方面的理论学说。

3) 他们能体会到编程的价值。

4) 他们擅长快速编程。

5) 他们是一个特殊程序的专家，能利用这些程序工作，比如 UNIX黑客（第一条到第五条是相互关联的，适合于这5条的人都属于黑客）。

6) 他们是某一种专家或狂热分子，比如有的黑客只热衷于天文。

7) 他们喜欢那些攻克或摆脱限制的智力挑战。

8)（这一条不是很被人认可）他们是一群恶意的干涉者，喜欢发掘四处寻觅发掘绝密的信息。比如“ 口令黑客 ”、“ 网络黑客 ”，不过这类人准确的定义应该是 cracker。

尽管媒体普遍认为闯入他人计算机系统或网络的恶意外部入侵者应该称作“ 黑客 ”，但上面的解释却表明，对于这类人的准确定义为 cracker。这个文件是这样定义 cracker 的：

他们破坏计算机系统安全，新闻报道中用 hacker来定义他们是错误的，后来又有人创造了“ worm ”（蠕虫）来定义他们，也是不准确的。这些新名词的使用在一定程度上也反映了人们对这类人的偷窃及破坏行为的反感。一个真正的 hacker可能会有一些无心的游戏性的破坏行为，而且他们懂得很多方面的基本技巧，除了出于一些实际的原因，任何过了初级阶段的 hacker们应该已经没有进行破坏的念头（比如，为了工作他们越过某些安全机制）。

hacker与cracker不能混为一谈，他们并不像一般读者所认为的那样有很多重叠的地方，这是受了想追求轰动效应的新闻媒体的误导。 cracker是一个很小、很紧密、很隐蔽的群体，他们与那些辞典描叙的庞大的公开的 hacker群体是不同的。尽管有时 cracker们也将自己描述成 hacker，但真正的hacker却认为他们自己是社会中独立的低层的一个群体。

抛开伦理道德不考虑， hacker们认为，不懂得开发想象力侵入他人的计算机系统，只会玩电脑的人，失落的东西太多了。

这些解释让我们了解到了黑客团体的一面。正如上文所说，这个团体中也有一部分不满于媒体所形容的“ hacker ”行为（比如网络破坏），他们也同样憎恶那些破坏电话网的人。这种行为被称为phreaking，其定义为：

1) 一种破坏电话网的行为和技术（比如，打免费长途电话）。

2) 广义上说，是破坏任何信息安全的行为（尤其是，但不是专指，破坏通信网络）。

曾经一段时间，phreaking在hacker中是一种半受尊敬的行为，他们认为 phreaking作为一种智力游戏，一种智力开发，是一项很好的活动，但盗窃别人的机密是应当禁止的。 hacker团体与那些利用类似于著名的“ TAP Newsletter ”的媒体来操纵半地下网络而破坏电话线路的顽固分子有很明显的区别。不过，在 20世纪80年代，当这种技术广为流传，并落入一些心术不正的phreaker手中后，情况变得不一样了。在这期间，电话网做了一些改进，那些老的用来破坏电话线路的技术不再象以前那样奏效了。因此 phreaker们开始了公开的犯罪活动，比如盗取他人的电话卡号码，像“ 414组 ”那样的犯罪行为使这种活动变得更为凶恶。现在仍有一些老的hacker们时不时地破坏电话线路，但现在已经很少听到以前 phreaker们时常携带的“ 蓝匣子 ”或者别的工具。

从这些文章我们可以明显看出，黑客团体也无法容忍那些恶意的外部入侵行为，他们为什么要这么做，他们的行为真的会构成威胁吗？要回答这些问题，你只需要到报刊杂志中阅读一下那些关于计算机系统和网络被入侵破坏的报导。尽管那些认为外部入侵行为将引发第二次世界大战的说法有些夸张，但这些行为确确实实会带来威胁。那些恶意的外部入侵者之所以要参与这种破坏活动的原因很难说清楚，因为原因太多了。有的人只是从中寻求刺激；有的人则是渴望因此而得到一个坏名声，尽管有时他们是匿名行为（通常破坏者在作案后会留下一个标记以此证明是他们干的）；还有的人则是因为一些意识形态或政治原因，只攻击某个特定的网站或留下某些特定的信息。这些恶意的外部入侵者有一个专有的术语定义他们： hactivist。他们是想尽一切可能的办法制造破坏，并希望自己的行为被人注意，但事后他们又想办法要证明自己的行为是合理合法的。

那些在网上进行破坏的hactivist，正如DefCon（在Las Vegas举行的一年一次的hacker大会）的一名发言人所评说的那样：“还没有想好理由就已选好了要攻击的目标。”

最后一种类型的恶意外部入侵者和那些受政府指派的间谍一样，都是罪犯，尤其是那些由有组织的犯罪集团支持的罪犯。这并不是一种新现象，早在 1995年，俄罗斯中央银行就宣称由于一项电子偷盗案，他们损失了超过二千五百亿的卢布。同样的事情也在美国发生过。 1996年，美国金融机构曾披露由于电子偷盗，他们每年都要损失八亿美元。由于 Internet的商业化以及网上银行和中介公司的激增，数据和电话网的犯罪活动也越来越多。

1.3 脆弱性

那么这些外部入侵和内部入侵是怎样完成的呢？为什么这些人能如此成功地破坏数据和电话网络的安全防护呢？第一个原因可能是由于控制网络的软件过于复杂。因此，有的错误不容易被觉察到，软件出现问题与技术的脆弱性有关，这些脆弱性可被人加以利用。即使在安全漏洞被发现后马上嵌入安全补丁，也会有别的脆弱性出现。这是一种永不停止的循环，任何新的软件或旧软件的新版本都会在不知不觉中给环境加入新的脆弱性。

许多已经发现的脆弱性问题并非只与安全漏洞有关，因为补丁是用来快速地解决问题的，而事实上有很多人从来不应用这些补丁，以至于自己的系统很容易受攻击。因为关于脆弱性的

信息到处都可以获得，比如安全补丁，那些蓄意破坏者懂得如何利用这些安全漏洞，他们所要做的就是寻找一个没有装入安全补丁的计算机系统。另外，安装系统时的错误的配置和系统管理员的粗心大意也会出现问题。比如，一些本该删除的错误的登录口令和访问密码被忽视了，没有删除。诸如此类的人为疏忽常常被cracker们利用。

另一个几乎在所有情况下都出现的脆弱性就是人的因素。假如哪一个hacker不能通过技术上的脆弱性获得访问权，他往往会想办法让别人告诉他登录的口令。这项技术，叫社会工程，十分有效。很多cracking组织都利用这一技术，如kevin Mitnick就常常运用这项技术，并且成功地达到了目的。一项非常奏效的反社会工程的技术就是专为职员们编的培训程序，帮助他们识别社会工程，并提醒他们如何遵循正确的安全规则。

电子设备存在的最后一个弱点，在行业中称为Van Eck现象，在军用方面称为TEMPEST。这些现象涉及利用电子设备产生的辐射进行监听。采用合适的设备，一个位于建筑物外面的人（通过一个指向建筑物的天线）便可以复制建筑物内部的某个人的计算机中显示的内容。幸运的是，能够精确地完成这件任务的设备是非常昂贵的，并且也非常容易屏蔽设备，使得辐射不容易被检测到。

1.4 使网络更安全的推动力

出于各种原因，我们要保护自己的网络，如果我们的计算机系统被入侵被破坏的话，所造成的经济损失是不可估量的。这一章前部分我们曾讨论过的民意调查已告诉我们如果数据网络安全被入侵破坏的话，所带来的潜在损失有多大。单说电话网络吧，每年要损失近十亿美元。

任何组织机构都愿意保护自己的网络不受潜在的损失，这是十分符合逻辑的。但令人惊奇的是事情往往不是这样的。许多机构会对自己的计算机和网络做风险分析。有人会觉得用来保护系统花费的成本太大，而系统遭破坏的可能性又很小，因此他们抱着侥幸的心理认为每年我们在民意调查中读到的那些灾难不会降临在他们头上。一直以来，怀有这种心理的人很多，但现在，其他一些因素改变了这些看法。

其中一个原因就是人们更加关心私人信息的保护，尤其是那些敏感的信息，比如医疗记录。对于这类案件，法律一律采取经济手段来进行惩罚。其实在有的案例中，当事人所犯的过错很小，可以也应该对其免除惩罚。以“HIPAA”法案为例，医疗信息原本是应该共享的，因此就需要一个安全可靠的计算机系统来确保它们既为所需要它们的人所享有，又要防止被无权访问它们的人接触。这项法案对蓄意入侵系统窃取信息的人和对那些粗心大意使破坏者目的得逞的人的处罚是一样的，既有民事又有刑事惩罚。

医疗卫生机构并不是惟一家已意识到要保护私人信息的组织。GLB法案（Gramm-Leach-Blighly）是为保护银行和金融机构而颁布的法案，该法案要求“确保用户记录及信息的安全性和保密性；防止任何破坏用户记录及信息的安全性和保密性的活动；防止对这些记录和信息的越权访问和使用，否则将会给用户造成伤害和不便。”总之，像GLB和HIPAA这类法案的目的是确定什么行为是对安全保护和行业的最好行为。这些法案还定义了最低层次的“due care”的含义。这有助于提高当局的官员们对电话和数据网络中的信息保护的重视程度。

第2章 安全要素

主要内容：

- 计算机和网络安全的基本因素
- 安全操作模式
- 安全投资的多种利益回报
- 分层安全

在过去的40年里，计算机安全的内涵已发生了相当大的变化。从20世纪六十年代后期到八十年代早期，计算机安全增添了一些新的内容，它包括对计算机硬件设备的维修保养，又包括计算机处理和存储信息的保护。对硬件的保护十分重要，因为硬件设备价格昂贵，而计算机本身的价值更是远远超出它所处理的信息的价值。只有保证硬件安全和可靠性，才能保证对计算机及其内部处理的信息的严格控制。

今天，基于两点原因，计算机安全的概念有所变化，人们不得不重新对计算机安全下一个定义。第一点，是因为出现了一些价格便宜功能强大的个人计算机和工作站，计算机硬件设备不再是最昂贵的设备，但计算机存储和处理的信息的价值却在不断提高。第二点是因为各种网络不断涌现，并相互连接，许多信息资源可以共享，不再简单地只受计算机物理存取的控制。

现在，计算机安全有时也指网络安全，但实际上它们是不同的两个概念。计算机安全专指对某一具体的主机的保护；而网络安全则指对所有相互连接的主机和流通于其间的信息的保护。这些单个的计算机相互连接组成了一个网络，因此任何一台主机在网上的行为和活动都应该属于网络安全的范围。对计算机硬件的维修和保护虽然很重要，但它已不是安全的首要任务。

今天，通过因特网和其他广域网，全世界的计算机用户都可以互联。虽然计算机系统和网络所运载的信息的价值远远超出了计算机硬件设备的价值，但拥有一套良好的硬件设备，确保系统运行的安全可靠性，可以大大提高我们的工作效率。更何况，这项工作不是很困难，花的成本也很小，除了对硬件的保护，我们还要考虑到组成计算机和网络安全的其他要素，如对信息资源的保护。

2.1 计算机和网络安全的基本要素

计算机安全包括三个基本原则或要素：保密性（Confidentiality）、完整性（Integrity）和可获得性（Availability），这三点就是我们常说的计算机安全的CIA。如果能达到这三个要求，计算机及其处理和存储的信息安全就有了足够的保证。

2.1.1 保密性

保密性是指，系统里的信息只对有权访问的人开放，这里所指的信息不仅包括存储的信息，还包括在网络上传输的信息。当越来越多的个人信息通过网络和计算机收集、存储并传输时，

保密性和个人隐私的问题也变得越来越重要。对于政府部门而言，保密性是保证其绝密信息不外泄的一个基本要素。

2.1.2 完整性

完整性指的是，只有有修改权的人或程序才能修改主机内的信息，网络信息也是如此。计算机的完整性有时也指，只有有权访问的人才能访问计算机内部的信息，因为没有授权的人一旦访问系统，就会很容易改变系统原来的状态。对于工业部门而言，尤其是金融业，完整性比保密性更为重要。比方说，一个入侵者即使知道某人在银行账户里的余额是多少，但他不一定知道怎样去修改这个银行账户。当然，保密性和完整性都很重要，只是对于工业部门而言，确保账户不被修改更重要些。但是，对于政府部门来说，保密性要重要些，因为它要保证国家的机密不外泄。

2.1.3 可获得性

和完整性一样，可获得性既适用于计算机系统，也适用于它所处理的信息。可获得性是指，当用户（或授权的程序）需要时，他能立即访问到所需要的信息或计算机及网络。

在计算机和网络时代初期，可获得性不是安全要素的一个内容，而是设备可靠性的一个指标。过去，计算机和网络常出现毛病，需要维修，这种事常有发生，使得用户们查不到需要的信息，给人们带来极大的不便。

随着计算机和网络的可靠性不断增强，人们希望它们拥有更多的功能，帮助处理一些日常工作。于是可获得性变得越来越重要。随着服务拒绝攻击的增多（详细介绍请见第 26章），可获得性逐渐变成安全的一个基本要素。

对于可获得性，数据网络和电话网络的要求稍有不同。如果计算机和网络因故障停机一段时间，我们似乎可以接受。但我们要求电话网络一直处于正常的工作状态。随着数据网络可靠性的增强及两个网络（数据及电话网）环境的交汇，人们对或获得性的要求更高了，希望它能达到电话网5个9的标准：99.999%。

2.1.4 安全破坏后的影响

如果三个基本要素中有一个未达到标准，会出现什么情况呢？假如保密性没做好，就意味着未授权的人或程序获得对信息的访问权，可能有人会访问你的银行账户，对你的收支了如指掌，或者你的绝密医疗记录甚至最近一次的物理考试成绩他也有可能知道。如果你在打电话，电话内容可能被人偷听（当然，随着无绳电话和手机的使用增多，这种情况的发生率会越来越低）。

保密性受损所带来的不仅仅是一些文件信息和谈话内容被窃取，有时信息及文件所处的环境也将被破坏。比如，你访问的某个网站或打电话的对象的所有信息都可能被窃取。这两种情况，你损失的不仅是部分信息的内容或结果，而是整个活动过程中的全部信息。

完整性受损，可能会导致某人或某个程序可以访问他本来无权访问的文件或系统，也就是说，我们无法再确保信息的真实可靠性，因为它们有可能不再准确。我们必须重装系统或应用软件，因为我们无法确保这些软件能否正常工作，也无法确保它们是否会执行一些多余的错误

的命令。电信网，尤其是收敛式网络，出现完整性受损的问题，可能是由于某人将输送中的信息包拦截后并做了一些修改，再将它们送到目标站。如果是这样的话，电话内容就被修改了，以致接电话的人听到的话并不是打电话人所说的。

可获得性受损，人们就无法得到想要的信息，情况严重的话，用户会对系统失去信心，甚至停止使用它。如果数据网和电信网相连，则数据网络上的服务拒绝攻击增多对电信网络也会构成一种威胁。当数据网和电信网建立连接时，对网络的可靠性要求更严格。如果系统无法抵制服务拒绝攻击，就达不到上文所提的 5个9的可获得性标准。如果谁想中断某个企业或组织的电信通信，他只需在网络上实施一次服务拒绝攻击，就能马上破坏其数据和电信网络。

随着网络服务的扩展，CIA模型出现了一定的局限性。它所描叙的网络安全基本要素并没有囊括所有的安全要素。在网络尤其是商业交易中，接收信息方必须要知道发送信息的是谁。比方说，一个公司接到一批订货单，它必须能确信真正发送订单的人或公司是谁。

2.1.5 验证性和非拒绝性

为了保险，我们引进了“验证性”这个术语。有的安全专业人士认为，验证性已包括在完整性要素中。他们认为：一个错误的信息（并非真正发送者传输过来的信息）是由于缺少完整性而造成的。这种说法有一定道理，但验证性之所以重要，在于它确保了信息来源的真实可靠，将验证性从完整性中分离出来，可以保证用户的合法身份。做到这一点，可比确保计算机的完整性要困难得多。

在电信网上，验证的方式有多种，呼叫 ID就是用来确认呼叫人的一种简单的验证技术。要使接电话的人在另一头听到的声音与说话人的原声相差无几，声音在传输过程需要一个标准声频。将声频保存在一定的带宽上并使其能保持一个可接受的声音复制，这是确定标准声频的基本要求。正常情况下，人们说话的声频约在 20Hz~20KHz之间，而在传输过程中标准声音信号的频率只有 300~3400Hz。早期电话专家们认为；在这个声频范围内，信号可以承载足够的能为接电话人辨别的声音量，这其实是一种验证的方法。只不过，当时并不是将它作为一项验证技术，而且是为了使电话中的谈话尽可能的趋向于生活中的谈话而已。

网络传输安全的另一个重要的要素就是非拒绝性。非拒绝性指的是：接受信息的一方不能拒绝接收传送过来的信息。这一点对于商业交易更为重要，因为公司必须确定对方已接收到传送过去的商业信息。尤其是中介公司对这一点要求更高，他必须在最短的时间内确定双方都已接到传输的信息（并确认收到的时间）。验证性和非拒绝性（以及其他的安全要素）确保了网上交易活动的顺利进行。

2.2 安全操作模式

以前，人们将网络与计算机安全工作的重点放在防御上，如果能阻止越权访问的行为，系统似乎就安全了（尽管有时也会因为某些中断，如电源、空调等，用户找不到需要的信息）。当远程终端技术引入后，计算机便可自动检验用户的身份。但防止越权访问，仍是安全工作的目标。

尽管科技发展取得很大进步，人们仍存在这种观念：“保护就是要防御”。当计算机在政府

部门日益普及后，人们越来越重视其系统的安全可靠性了。于是，国家计算机安全中心（国家安全局的一个组成部分）专门撰写了一套取名为“彩虹”的系列丛书（因为书本的颜色为彩虹的七种颜色）。

该丛书的基础入门篇《Trusted Computer System Evaluation Criteria TCSEC》，即橘黄色封面的书，列举了一系列评判计算机安全的标准，这些都是20世纪80年代国防部用于评判网络系统是否安全的标准。但TCSEC并未提出针对一些新出现的网络安全问题的解决方法。于是国家计算机安全中心又出版了另一本红色封面的书《Trusted Network Interpretation（TNI）》，该书将TCSEC中计算机安全评判标准运用于网络环境中，并介绍了一些TCSEC中未涉及的具体的网络安全评判标准。这两本书主要告诉人们如何防止入侵者越权访问系统和数据。

这套彩虹系列丛书是联合国国防部的一组文献资料。除了联合国国防部，其他一些国际组织也制定了有关计算机和网络安全的评判标准。一时间，纷繁杂乱的安全评判标准引得厂商们怨声连连，因为他们的产品在各国销售前要经过层层审查和鉴定（至少要经过政府机关的检查）。最终，一个统一的安全评判标准应运而生，并为大多数国家承认。但所有这些标准都存在着一个问题，它们仍是防御性质的。

“防御即保护”模式存在的问题中，无论你的防御范措施怎样完善，总会出现问题和差错，导致泄密事件发生。我们可以拿二战前法国的马其诺防线作类比，解释这个问题；法国人修造了一条坚固的防线，用于抵御德国的进攻，在当时法国军方的高层人士看来，这道防线绝对是坚不可摧的。然而，德国的总参谋部决定绕过这条防线，不采取正面攻击。法国人原本想利用这道防线将德军阻隔在国界线外，他们万万没想到事情的结果会是那样。网络安全的情况与之类似。无论安全人员设计一套多么完善的防御装置来阻止入侵者访问；他们还是会找到一个避开防线绕道进攻的方法。就像法国军队一样，当灾难来临时，安全人员毫无准备，计算机和网络安全就会受到巨大威胁。

最好的办法就是要在事情发生之前有所觉察并进行检测，事情发生后，能迅速检测并寻找到问题的所在，这就是我们说的计算机安全操作模式，可以用下面的公式表达：

保护=防御+（检测+反应）

这个模式最早在空军战争情报中心于20世纪80年代末90年代初提出，该中心位于得克萨斯州的圣安特尼奥镇（San Antonio, Texas）。我们注意到了，防御仍是这个模式的重要组成部分：我们仍要防御入侵者对系统的访问，这是首要工作。我们已经认识到，无论在防御上作了多大努力，入侵事件仍会不可避免的发生。因此，操作模式与以往的模式不同就在于，除了防御，我还要做好当系统被入侵后，要尽快进行检测并随时作出反应。安全操作模式的发展带来了一些新技术的发展，比如入侵侦察系统（见24章）。

对于侦察，操作模式的一个重要环节就是对计算机和网络安全状态的连续监控。同样也是空军战争情报中心首先提出，安全是一个持续不断的过程，它要求随时制定并调整安全策略，这样才可以随时检测到出现的安全缺口，图2-1可以帮助理解操作模式这一连续的性质。

这个持续的状态过程有多种划分，大多数划分方式都用一个如图2-1的车轮表示，只是划分的扇区数量从3到5个不相等而已。有的划分图没有被其他部分包围的中间环节，它表示度量，用来衡量每个扇区的地位。

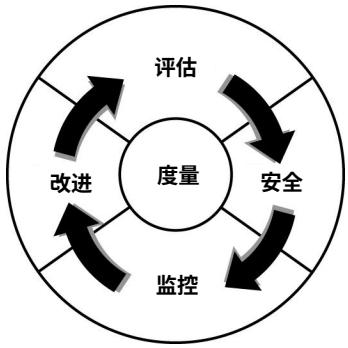

图2-1

通常，首先完成的环节是评估扇区，这是这个过程的开端，在这一环节中，计算机首先对网络安全状态进行检测，查找出存在的安全缺口，并决定下一步的对策，然后采取相应的安全策略和程序帮助保护系统的安全环境。这个环节中，一般的任务就是风险分析或脆弱性评估。

在安全扇区中，计算机继续执行安全方案和程序，启动装配的安全基础设备。网络的安全方案包括以下安全产品和技术：防火墙、加密术、虚拟专用网络、存取控制设备和入侵侦察系统，这些设备组成了操作模型中的防御和检测部分，检测技术又直接服务于下一个环节，监控扇区。

在监控环节中，计算机不断对网络安全状况进行检查，看当前情况是否正常，是否有入侵攻击行为出现。通常，一个管理安全服务的供应器可同时为电话和数据网络提供 24-7监控。虽说度量在整个过程中都很重要，但对于监控扇区，它尤为重要。如果计算机不知道寻察的目标是什么，也不知道什么是网络安全的正常状态，那么它就无法确定网络是否安全，是否发生了攻击事件。度量可揭示当前安全防护中存在的问题，也为以下最后一个环节，改进扇区做准备。

监控扇区所发现的安全缺口是改进扇区执行任务的根据。安全设计检查程序根据当前安全标准来决定安全缺口所处的当前位置，最近常出现的新的脆弱性及最佳的解决途径。根据新的脆弱性或风险评估，计算机采用相应的安全基础设备和安全策略。改进环节也是一个持续不断的过程，因为网络的安全状况瞬息万变，系统要随时进行评估和脆弱性检测。

度量用于确定网络安全与否，或衡量当前网络状态，它对于侦察检测反常状态和入侵活动具有重要意义。当前监控的资料和存留的历史信息都十分有价值。比方说，在一周内发现系统被探测的次数高达2000次，这是否暗示着有潜在的入侵行为呢？如果以往正常情况下，每周被探测的次数只有100次，则答案是肯定的，如果有1950次，这与正常情况的次数大体相近，则说明网络基本上是安全的，但这个数据仍具有意义，虽然它并非暗示着一定有入侵活动。

保留的历史信息可以帮助做出重要的预测，但对于安全人员来说，不能因此而满足，还应该小心谨慎。上文所举的事例中，每周发生 2000次被探测的事情，不管这个数字是否符合正常状况下的标准，它都具有重要意义。通过将它与用其他方法得到的数据对比，可以确定这个数字是否有价值，能否说明什么问题。这个数字超出以往正常状态下被探测的次数，可能说明有入侵行为，但即使在正常的次数范围内，也不会说明，网络是绝对安全的。

不同的企业或单位，具体的衡量标准是不同的，这很大程度上取决于企业或单位的性质。

普遍的判断标准包括：

登录失败的次数 一般情况下，登录失败的次数是基本不变的，有时多多少少会有些变化，尤其是雇佣了新职员或用户被迫改写原来的登录口令，但这种变化的差距并不大。如果发现相差的次数太大，则说明有入侵者试图猜测登录口令。因此，我们应该经常地统计一下登录失败的次数，注意那些时常登录不上的账户。管理员或底层经常登录不上的账户有可能已被入侵了。

网络被扫描或探测的次数 入侵者经常会扫描网络。如果发现被扫描的次数突然增多，则可能说明系统出现了一些新的脆弱性，并且有人持续地试图进入系统，试图窃取系统的信息，将这个数字与以往被扫描次数相对比，就会知道，可能有人在寻找计算机的脆弱性。

目标对象访问失败 用户可能会定期访问一些未授权访问的文档，如果访问失败和次数增多，尤其是对某个用户如此，可能说明了是一个新用户漫游于系统内，也可能说明该账户被人盗用，成为入侵者进行破坏活动的据点。跟登录失败一样，我们也要经常性地对目标访问失败次数进行统计。

登录口令被修改 管理员应该时常修改计算机和网络的登录口令，以保证用户不选择过于简单容易被猜中的口令。如果容易被修改的口令增加，则说明需要加强安全培训，只有经常的修改口令，用户们才注意选择合理的登录口令。

短促的电话呼叫次数 如果电话铃经常响，而且每次响声又很短，可能暗示有入侵者试图在你的企业或单位安装调制解调器。每月，可能会因有些人错误地访问系统而造成这类事件的发生，但如果在一个短时期内，发生的次数增多，则说明有入侵活动。如果只是一台电话发生这种毛病，有可能是当地因特网服务供应器的号码与该机相似，或是某个粗心的用户拨错了电话。

长途呼叫次数 如果你企业或单位的长途电话增多，有可能是PBX受到入侵威胁，尤其是在周末或下班后，长途电话呼叫增多，这种可能性更大。国际长途增多也可能意味着同样的入侵行为。

接收和发送的电子邮件数目 如果某个时期，电子邮件数增加，尤其是大量增加，比如电子邮件增加了十倍，则有三种可能：也许是节日期间，用户们向亲朋好友问候祝福；也许是电子邮件病毒发作；也许是系统受到服务攻击。如果存在电子邮件病毒，企业或单位受到服务拒绝攻击，邮件数会在短期内急剧增加，正常的网络管理行为可以检测到这样异常现象。

从上文的例子我们不难发现，企业或单位可以采用不同类型的度量标准来监控本组织的计算机或网络安全状态。有的变化在短期内就会被察觉（如电子邮件病毒发作时，电子邮件数目的变化），但有的变化要经过很长一段时间才会被发现（如被扫描或探测的次数）。对网络的监测可以帮助确定异常现象发生的时间，当然一些能明显影响网络反应时间的活动除外。即使网络的执行功能受到影响，其灵敏的监控能力仍可以在危机发生之前准确的察觉到异常的变化。

理解计算机安全操作模式，还出于另一个原因。为了检测以及对安全事件做出反应，网络应同时具有可见度和控制能力。网络（无论是数据网还是电信网）的可见度可以帮助管理网络的日常操作，而控制能力则可对安全事件做出及时准确的反应，帮助加强网络控制。网络的可见度和控制能力，使得某些操作问题解决起来不那么困难了，如资源利用。这一点意义十分深远，因为这意味着安全被加入到每天的日常管理工作中，而不是一项附加的任务。这一点并不为大多数企业和单位所理解，因此，许多人还在为他们的安全问题发愁。其实，那些对安全工

作已经予以重视的企业和单位也并没有把网络的安全作为一项应做的工作，只是把它当成一个保险的机会，其实，对安全的投资并不是万本无利的事情，有时你会因此得到巨大利益回报。

2.3 安全投资的多种利益回报

安全工作需要投资，但你会因此而获得很多回报。每一个企业和单位，对不同的工作任务编制预算，比方说对信息技术的预算，可能会占整个企业预算总额的 3%到6%。通常安全工作上的预算开支来自于这笔经费，并只占其中的一小部分，也就是整个企业预算总额非常非常小的一部分。

其实，以往信息技术上的预算并没有占到预算总额的 3%到6%，只是因为现在信息技术的价值大，能为企业或公司带来巨大经济利润，所以对它的投资也就大了。只要在信息技术上花一点成本，你就能节省一大笔别的花费。比如说，采用新技术，可以雇佣少一点人力，同时工作效率也会提高。这种在时间和人力上的节约就是金钱上的节约，节省的时间又能用来创造更多的财富，带来更大的利益回报。与此相似，在安全工作上投资一点，你同样可以收回更大的利益。

这些利益并不完全是经济上的利益，它包括：

- 计算机和网络的安全保障
- 提高网络安全性能
- 节约预算支出
- 增加额外收入

安全人员认为，投资配置安全产品和安全程序，可以保证企业或单位的网络安全，这才是最大的利益回报，因为这样可避免安全事故的发生及其带来的巨大经济损失。第 1章中的资料显示，一次事故带来的潜在损失很大，包括企业或组织独有的信息资料，软件产品及生产力等都可能受到影响。这种情况下的利益回报并不能直接的创造经济财富，既不产生额外收入也没有节约其他预算。

另一个回报即提高网络的安全性能，某些安全产品和程序功能宣称自己比其他的安全产品和程序要强大。这就好像媒体中可乐或清洁剂的广告大战，某种清洁剂可能会宣称，它能使衣服洗得更干净，使色彩更鲜亮，人们想使衣服洗得干净光洁一些，就会受诱惑去买这种清洁剂。同样的，入侵侦察系统也会宣称它在探测安全问题方面比别的系统要强。安全人员当然更想查找出尽可能多的安全漏洞，于是他们就会购买这种产品，这种类型的安全产品可能不能带来额外收入，但可以节省其他预算，恰好与其成本花费相抵消。

有的产品确实能带来经济利益，如节约预算。如果节省的钱比购买这些产品的成本要多，则可以说，这些产品实现了其价值。防火墙和入侵侦察系统就是很好的例证。这些工具都可使网络具有可见度和控制能力，同时显示哪些资源利用是一种浪费。比如通信防火墙，它可以显示哪些线路不需要开通，或告诉你用于传真的线路比实际所需的线路要多。撤消这些多余的线路，便可以节省一笔开支，这就是安全产品所带来的直接回报。其实，任何一个企业或单位都会遇上这种情况。

最后一项，就是由于安全产品而创造出实际收入。一般的安全产品都不会直接带来收入的

增加。网上银行和中介公司，离不开网络安全产品，否则它们就无法开展正常的交易活动，创造不了生产价值。除此之外，大多公司不会因安全投资而带来直接的经济利润，最多不过是节约其他预算开支。

明白了安全投资带来的不同经济利益回报，有助于某些人计算这种投资是否合理，并能使安全人员对那些购买安全产品的决策人员做出合理的建议。仅仅考虑到投资带来了网络安全，投资者会感到这并不合算。但看看它带来的其他经济利益，投资者就会觉得花在用于保护数据和电信网的钱是值得的。

2.4 分层安全

人们在讨论编制一个有组织的安全程序时，常常会提到分层安全的概念，这种想法就是要在网络周围安装多个防护层，以增加入侵难度，保护网络安全，这即可适用于独立的电信和数据网，又可以应用于电信和数据网会敛而成的新型网络中。

分层安全的想法很有价值，因为它还可提供一个粗略的指示图，帮助决定采用哪种安全产品和安全对策。每通过一个安全层，入侵者得逞的机会就少一分，也就是说，每多一个安全层，就少一批入侵破坏分子。低层中的一些安全产品和技术可以防止大量入侵行为，避免大的经济损失，以下是各层中使用的不同网络技术。

1) 防火墙
2) 虚拟专用网络
3) 访问控制设备
4) 入侵检测系统
5) 网络扫描设备

有的人认为这种排序方法不科学。有些处于基础地位的产品或技术应该放于更高的安全层，这种想法有一定道理，但更重要的是要形成一个有组织有系统的方案来保护网络。很多人认为，防火墙是最简单的安全产品，但它限制入侵者越权访问的能力最强，所以任何一种网络安全分层方案都应该把它放在最基础的位置。不幸的是，有的网络常常只建立一个安全层，即防火墙，因为它能对各种安全现象作出及时反应，有的企业和单位就仅仅满足于此了。

上文所说的安全分层方案中列举的各种技术，既适用于数据网络又适用于电信网络，有的计算机管理员会在一个网实施安全防护之前，在另一个网络设置所有的安全层，这是十分危险的。因为其中一个网是完全开放的，为入侵者入侵另一个网提供条件，用调制解调器将数据网与电信网相连接，就会出现这种现象。因为电信网没有配置完善的安全设备，攻击者可以利用调制解调器入侵数据网。因此电信网和数据网必须同时装上防火墙，才能消除威胁。只有两个网络同时受到保护，安全分层才有意义。随着数据网和电话网会聚技术的发展，两个独立的网络安全层也会会聚形成一个统一的安全层。

2.5 结论

对于电信网和数据网而言，他们的基本安全要素是相同的。保密性、完整性和可获得性，即常说的网络安全CIA，一直都是安全组成的三个基本要素。随着网络的发展，尤其是网络的商

业用途增强，验证性和非拒绝性也会成为基本要素之一。

保护网络安全的方法有很多种，早些年，对网络和计算机的保护就是要防御进攻。但这种模式存在明显的不足之处，因而操作模式应运而生，它增添了检测和反应两个环节。同时，操作模式使用了安全防护层次，在每一个层上都配置不同的安全技术和安全产品，用以阻挠入侵者的破坏活动，增加其入侵难度。

最后值得一提的是，网络安全投资总被认为是一件万本无利的事，而最近的一些技术促进了在企业运作中使用安全技术，这些技术表明网络安全投资同样可以带来巨额利益回报。这对企业的领导者来说，的确是一件值得庆贺的事，他们再也不会对网络安全投资是否合算产生怀疑了。