JISUANJI WANGLUO
ANQUAN JISHU YANJIU

计算机网络安全技术研究

蒋建峰 著

苏州大学出版社
Soochow University Press

计算机网络安全技术研究

蒋建峰 著

苏州大学出版社

图书在版编目（CIP）数据

计算机网络安全技术研究 / 蒋建峰著. —苏州：苏州大学出版社，2022.2
ISBN 978-7-5672-3849-7

Ⅰ. ①计… Ⅱ. ①蒋… Ⅲ. ①计算机网络—网络安全—研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2022）第 013360 号

书　　名：计算机网络安全技术研究
著　　者：蒋建峰
责任编辑：征　慧
装帧设计：吴　钰
出版发行：苏州大学出版社（Soochow University Press）
社　　址：苏州市十梓街 1 号　**邮编**：215006
印　　刷：镇江文苑制版印刷有限责任公司
邮购热线：0512-67480030
销售热线：0512-67481020
开　　本：787 mm×1 092 mm　1/16　**印张**：10.75　**字数**：211 千
版　　次：2022 年 2 月第 1 版
印　　次：2022 年 2 月第 1 次印刷
书　　号：ISBN 978-7-5672-3849-7
定　　价：56.00 元

图书若有印装错误，本社负责调换
苏州大学出版社网址　http://www.sudapress.com
苏州大学出版社邮箱　sdcbs@suda.edu.cn

前　言

信息、材料、能源已成为人类社会生存与发展的三大支柱和重要保障。信息技术的快速发展给人类社会带来了深刻的变化。随着计算机网络技术的飞速发展，我国在网络建设方面取得了显著的成就。随着电子银行、电子商务和电子政务的广泛应用，计算机网络已经渗透到国家政治、经济、文化和国防建设等领域，并已遍布现代信息化社会工作和生活的各个层面。“数字化经济”和全球电子交易一体化正在形成。计算机网络安全不仅关系到国计民生，而且与国家安全密切相关。网络技术中最关键、最容易被忽视的安全问题关系着网络系统的健康发展和应用。随着计算机网络的广泛应用，网络安全技术和应用越来越受到世界各国的关注。

日常活动和商业活动对互联网的依赖程度越来越高，因而人们对网络工作的安全性提出了更高的要求。例如，严格控制对网络资源的访问，防止计算机病毒和非法入侵者的破坏。本书旨在对计算机网络安全管理技术和安全检测技术进行研究，提高网络系统数据的保密性、完整性和可用性，保障网络系统的服务和审查，确保网络系统的硬件、软件和系统中的数据资源能够完整、准确、连续地运行和服务。同时，本书还为及时修改和优化网络配置、提高运行效率、消除网络通信瓶颈提供了相关技术与方法。

在本书写作过程中，作者参考和引用了国内外学者的相关文献，在此一并表示衷心的感谢。

由于作者水平有限，书中错误和遗漏在所难免，敬请各位同行和广大读者批评指正。

目 录

第一章　计算机网络安全

第一节　计算机网络安全的基本概念

一、计算机网络安全的定义

计算机网络通常是指能够实现信息传输及资源共享的一种计算机系统。计算机网络系统一般可分为网络硬件和网络软件。网络硬件由主体设备、连接设备和传输介质三部分组成。网络软件包括网络管理软件、网络操作系统及通信协议，基于这三者的管理和协作，才能实现资源和信息的传输与共享。在连接不同地域、不同数量的计算机时，只有将通信线路作为主要的辅助工具，才能将多台计算机实现外部连接，并且在连接之后体现出每一台计算机的独立功能。

本书从以下两个方面来阐述计算机网络安全的概念：一是计算机网络系统安全，二是计算机网络信息安全。计算机网络能够向计算机用户传输信息资源，并且为其提供服务。基于计算机网络这样的特性，我们可以从安全的角度定义计算机网络：所谓的计算机网络安全，指的是能够在网络体系中确保服务，在信息传输的基础上具有极高的可用性，以及在网络体系中资源信息能够保证高度的完整性。

可用性对计算机网络提出的要求是，基于用户在计算机网络中的需求，能够为其提供不受时间、空间限制的网络服务，满足用户随时随地对信息资源的使用所提出的要求。

完整性对计算机网络安全提出的要求是，在用户使用网络服务的过程中，能够确保这些信息资源的准确性及保密性。另外，要确保用户使用的这些信息是完整的，并且存在的信息是可用的。

由此可见，现阶段计算机网络安全需要解决的一个问题是，如何能够在安全的网络系统中，为用户提供一个范围合适、类型适当的网络服务。与此同时，还要确保外部连接的每一台计算机，都具有高度的可用性及连通性，

从而使网络用户在使用网络服务时，能够得到可用性和完整性极强的资源信息，这也是对网络系统的一种保护。

综上，可以看出计算机网络安全不仅仅涉及技术方面的问题，也会涉及一些管理方面的问题。在计算机网络安全工作中，需要二者协同，才能够对网络信息进行保护。从技术的角度来看，技术主要的作用是阻止计算机外部一些非法用户对计算机网络系统的恶意攻击；从管理的角度来看，管理的作用更侧重于计算机网络安全系统工作内部的人员管理，从人为因素方面去规避一些问题和矛盾，以此来保护计算机网络安全。

二、计算机网络安全的特征

实际上，计算机网络安全属于综合性比较强的一门学科，内容宽泛，不仅涵盖计算机科学、计算机网络技术、密码技术与信息安全技术等方面的内容，还涉及应用数学及信息论等学科的内容。

计算机网络安全所要保护的对象有硬件设备、软件设备及数据资源等。在保护计算机网络安全的过程中，需要做到的是以上这些保护对象不会遭到外界的恶意破坏，数据资源不会被篡改或者被泄露，这样才能确保计算机网络的正常运行。同时在计算机网络系统运行的过程中，要保证其具有较高的可靠性，最重要的是能够为网络用户提供可持续性较强、不会轻易间断的网络服务。计算机网络中的所有信息都是具有保密性和完整性的，在使用网络信息的过程中，这些信息具有可靠性和真实性。在网络安全管理的过程中，所有能够与这些网络信息特性相关联的管理工作和技术工作，都属于网络安全领域需要研究的内容。

（一）计算机网络安全的特点

通俗地说，网络信息安全与保密主要是指保护网络信息系统，使其没有危险、不受威胁、不出事故。从技术角度来说，网络信息安全与保密的目标，主要表现在系统的保密性、完整性、可用性、可控性、可靠性、不可抵赖性等方面。

1. 保密性

保密性一般是指在计算机网络安全系统中的信息资源不被泄露给非授权的用户、实体或过程，或供其利用的特性。针对网络信息的保密性，常用的几种安全措施有：对网络信息进行物理安全管理；针对一些比较重要的信息资源进行加密处理；适当地进行监控防护和核辐射防护；等等。

2. 完整性

完整性指的是其信息资源未经授权不能被擅自篡改和更改的特性。也就是说，网络信息在传输和存储过程中保持不被伪造或者删除，也不会在使用的过程中出现重播、乱序及插入等的特性。影响网络信息完整性的主要因素有计算机硬件设备出现故障，软件环境中出现代码错误，计算机系统中出现病毒或者存在外界的人为攻击行为等。

3. 可用性

可用性指的是在信息资源使用的过程中，允许授权用户或实体正常访问的特性。也就是说，计算机网络信息系统中的资源，能够为被授权的用户提供正常的信息资源服务。网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的，有时还有时间要求。已经被授权的用户，在访问网络信息资源时会进行身份识别和确认，这样才能够针对被授权的用户提供访问权限之内的信息资源服务。

4. 可控性

可控性是对网络信息的传播及内容具有控制能力的特性。即被授权的用户可以按照自己的需求随时随地地在计算机网络中使用自己所需要的信息资源。可控性要求计算机网络信息系统能够对被授权的用户提供即时性的信息资源的传输。

5. 可靠性

可靠性是系统安全中最基本要求之一，它是指在整个网络体系中，无论是原软件的运行还是硬件的运行，都需要保证其自身具有无故障的特性。可以从以下几个方面来提高计算机网络信息系统的可靠性：不断提升计算机网络信息系统硬件设备方面的质量；在配置方面做好备份工作；针对故障及时地进行纠正和自我修复；制定容错措施；从科学合理的角度去分配运行过程中的负荷问题；等等。

6. 不可抵赖性

计算机网络信息系统还具有不可抵赖性，我们也常常将其称作不可否认性，这一特性常出现在信息资源的互换过程中。基于这样的特性，能够使计算机网络信息资源在交换的过程中，双方的参与者都不能对操作进行否认和抵赖。简单来说，这种特性与签名、签收等形式有一定的相似性。

（二）物理安全

1. 防盗

和其他物品一样，计算机也是盗窃的目标。计算机的流失所造成的损失

远远高于计算机硬件本身的价值，所以在日常工作过程中，针对计算机的防盗工作要做好合理的预防措施。

2. 防火

在物理防护方面还要注意防火。通常情况下，计算机机房出现火灾的原因有以下几个方面：电气方面出现了问题；人为的火灾事故；外部环境中的火灾蔓延到计算机机房，导致机房发生了火灾。

① 电气方面，可能会出现的问题是：设备和线路出现接触不良或者短路；静电及绝缘层遭到破坏；信息量负荷过大；等等。

② 人为事故方面，多数是机房工作人员操作不当引起火灾，如在易燃物较多的地方吸烟或者乱扔烟头等，也不排除会有人为纵火的情况。

③ 外部环境中的火灾蔓延，通常是指计算机机房以外的空间结构中出现了建筑物方面的火灾，火势扩大蔓延到计算机机房，从而引起连续性的火灾。

3. 防静电

静电在我们日常生活中很常见，是两个物体之间摩擦或者二者相接触引起的一种现象。在机房，计算机的显示器会产生非常强的静电，如果没有释放出去，那么这种静电就会在设备或者物体中停留，其自身的势能是非常大的。由于放电会产生火花，这些火花很有可能引起火灾，一旦发生火灾，就会对机房内的大部分集成电路造成不可逆的损坏。

4. 防雷击

随着科学技术的发展和电子信息设备的广泛应用，对现代防雷技术提出了更高、更新的要求。采用传统的避雷针，不仅不能满足微电子设备的安全需求，还会带来很多弊端，如增加了被雷击的概率、产生感应雷击等。而感应雷击是损坏电子信息设备的主要杀手，也是易燃易爆产品着火的主要原因。

5. 防电磁泄漏

有一些电子设备会在工作的过程中出现一种电磁辐射的情况，比如计算机在工作过程中就会产生电磁辐射。计算机的电磁辐射可以从两方面来概括：其一是辐射发射，其二是传导发射。在计算机工作的过程中，无论是哪一种形式的发射，都会被灵敏度较高的接收机所接收，进而对其进行有效的恢复和分析，这一过程中会出现电磁泄漏的情况。

（三）逻辑安全

一般情况下，计算机逻辑安全的实现方法有以下三个方面：一是密码权限；二是文件权限；三是审计工作。如果想要在计算机正常运行的过程中有效防止黑客的一些恶意行为，那么就需要做好逻辑安全方面的防护工作。

用户可以通过限制登录次数或者限制操作时间来确保逻辑安全。储存于计算机档案内的资料可由软件加以保护，该软件限制存取他人拥有的档案，直到该档案的拥有者明确准许他人存取该档案为止。另一种限制访问的方式是通过密码，计算机在接收到访问请求后要求检查密码，然后在访问目录中匹配用户账号和密码。此外，还有一些安全包可以跟踪可疑的、未经授权的访问尝试，比如多次登录或对他人文件的请求。

（四）操作系统安全

在计算机网络信息系统中，最基本也是最重要的一个组成结构就是操作系统。一般情况下，同一个计算机系统能够供给多个工作人员或者用户同时使用，为了保证计算机操作系统本身的安全，要在构建系统的同时考虑到用户的需求。只有做好系统分区，才能够确保用户在正常访问网络系统的时候，只在自己的访问区域操作，而不会涉及或干扰到其他的用户。例如，大多数用户操作系统不允许一个用户删除属于另一个用户的文件，除非另一个用户明确地给予许可。

不同的操作系统，在功能和安全性上也有很大的差别。通常情况下，功能比较强大、安全级别更高的操作系统能够为系统中每一个用户设置个人账号。一般情况下，每一个用户只能操作属于自己的账号信息，操作系统本身是不允许已经注册的账号去恶意修改另外一个用户的账号信息的，也就是说除了自己本身的信息数据之外，他人的信息数据是不可以被更改的。

（五）联网安全

计算机网络系统在联网的过程中需要保持高度的安全性。安全性之所以能够得到保障，是通过安全服务来实现的。具体的安全服务分为以下两种：

第一，访问控制方面的服务，其目的是使计算机联网之后的信息资源得到正常授权才能被使用，即确保信息资源不会出现被非授权用户使用的情况。

第二，通信安全方面的服务，其目的是使联网之后的数据信息，自身的完整性和保密性得到进一步的确认，以确保通信过程中所有的信息资源具有可靠性。

例如，因为电子商务基于互联网结构，所以电子商务就需要在联网的过程中广泛地应用通信安全服务。

三、计算机网络安全层次结构

开放式系统互联（open system interconnect，简称 OSI），一般称作 OSI 参

考模型，是由国际标准化组织（international organization for standardization，简称 ISO）颁布的，提出这一模型的目的是使设备在网络互联的过程中有一个标准的参考框架。TCP/IP 参考模型在开放式系统互联参考模型的基础上，分成四个不同的层次：网络接口层，这一层所对应的是 OSI 参考模型中的物理层和数据链路层；网际互联层，这一层所要面对的是通信方面的问题，也就是需要解决连接的主机之间通信方面出现的一些问题，与之对应的是 OSI 参考模型中的网络层；传输层，对应的是 OSI 参考模型中的传输层，这一层的具体功能是将端到端的通信功能落实在具体的通信工作中；应用层，与之对应的是 OSI 参考模型中的高层，这一层的主要工作任务就是以客户的需求为主，为其提供多元化的应用服务。

从网络安全的角度来看，参考模型的每一层都可以采取一定的安全手段和措施，提供不同的安全服务。但是，单个层次不能提供所有的网络安全特性，每个层次必须提供自己的安全服务，共同维护网络系统中的信息安全。

在物理层，可以在通信线路上采用电磁屏蔽、电磁干扰等技术，防止通信系统以电磁的形式（电磁辐射、电磁泄漏）向外界泄露信息。

从数据链路层来看，加密工作是针对数据链路通道，在电路上通过加密机制进行通信加密。在信息离开某一台计算机之前就可以对其进行电路上点对点的信息加密，也可以在信息进入另一台机器的时候，对其进行链路上的点对点加密。这一加密过程中涉及的细节，都是建立在计算机硬件底层的基础上，通常情况下在上层结构中是不能实现的。

从网络层来看，针对处于网络边界的一些信息资源，其安全工作需要通过防火墙技术来处理，这样就需要确定信息是来自哪一个源地址，之后要确定的是这一信息对主机有没有访问的权限，这样就能够确保在信息网络体系内，主机不会被非法用户进行恶意访问。

从传输层来看，信息流的安全工作，可以用端对端加密的形式来实现，也被称为进程到进程的加密。

从应用层来看，安全工作主要针对的对象是用户身份上的甄别，需要进一步认证和确认访问者的身份，才能够提供安全性较高的通信渠道。

四、计算机网络安全的责任与目标

（一）计算机网络安全的责任

从高级管理者到日常用户，很多人员都能在计算机网络的安全建设中发挥作用。高级管理者负责推行安全策略，其准则是“依其言而行事，勿观其

行而仿之”，但是源自高级管理者的策略和规则往往会被忽视。用户不仅要意识到网络安全的重要性，还要意识到不遵守规则可能会带来的后果。一个很好的方法是提供短期的安全培训课程，让人们可以提出问题和讨论问题；另一个比较好的做法是在经常出入的公共场所和使用场所张贴安全警告（如网吧、机房等）。

（二）计算机网络安全的目标

计算机网络安全的最终目标是利用各种技术手段或者工作管理手段，确保网络信息系统在运行过程中能够具有保密性、完整性、有效性等。

1. 保密性

网络信息系统具有保密性，意味着信息系统结构中的信息资源在运行的过程中不存在非法泄露（或者能够具备有效防止自身信息泄露这一特性）。通常情况下，信息系统中的资源、访问的权限仅提供给已被授权的用户。

信息资源的保密性是通过多种技术手段实现的，其中包括对信息资源的加密、对访问者身份的验证、对访问时间及访问次数的控制以及网络安全信息通信协议等。

在信息资源防泄露的实现手段中，信息加密是非常基础的一项技术。在大多数情况下，计算机网络信息安全防护系统的主要防护结构都是由密码技术来实现的。也就是说，如果密码技术一旦泄露或者密码泄露，就会出现安全系统崩溃的情况。机密文件和重要电子邮件在 internet 上传输也需要加密，加密后的文件和邮件如果被劫持，由于没有正确密钥进行解密，劫持的密文仍然是不可读的。此外，机密文件即使不在 internet 上传输，也应该进行加密，否则窃取密码后就可以获得机密文件，对机密文件加密可以提供双重保护。

2. 完整性

信息完整性是指信息的可靠性、正确性、一致性，只有完整的信息才是值得信赖的信息。完整性与保密性不同，保密性强调信息不能被非法泄露，而完整性强调信息在存储和传输过程中不能被意外或故意修改、删除、伪造、添加、破坏，并且在存储和传输过程中必须保持不变。影响信息完整性的因素主要有硬件故障、软件故障、网络故障、灾难事件、入侵攻击和计算机病毒。确保信息完整性的技术包括安全通信协议，一旦信息遭到恶意破坏或者出现缺失，那么最有效的恢复方式就是数据备份。

3. 有效性

根据用户的不同需求，为用户提供数据信息访问服务，这一过程中展示

出的特性就是信息资源的有效性，这种特性对于用户来说是计算机网络信息系统所能体现的安全特性。一般来说，若网络信息系统能够满足保密性、完整性和有效性这三个安全目标，则可以认为信息系统在一般意义上是安全的。

第二节　计算机网络面临的安全威胁

一、影响网络安全的因素

（一）技术因素

从技术因素的角度来看，对网络安全造成影响的有计算机网络系统硬件上存在安全缺陷、软件上存在安全漏洞以及系统的安全配置策略等方面。

1. 计算机网络系统硬件上存在安全缺陷

不可否认的是，现阶段无论是从理论角度还是技术层面来看，计算机网络系统硬件都存在一定的局限性，这些因素就会使计算机本身或者计算机系统的一些硬件设备在运行过程中出现不同类型的问题，也会出现一些功能上的不足，从而在计算机网络系统的使用过程中就会存在较大的安全隐患。

2. 软件上存在安全漏洞

实际上，工作人员会在软件系统的后台留一个“后门”，这个“后门”的作用就是为了在日后的工作中不断地对其进行升级和改进。可是这也存在一些弊端，如果计算机网络被恶意访问或攻击，就会造成整个系统的崩溃。

3. 系统的安全配置策略

我们可以从常用的系统中看到默认设置，它所代表的实际上是较低的一种安全级别。另外，如果在网络配置上出现错误，那么就会存在一定的安全问题，也会出现一些安全漏洞。例如，系统中的密码文件并没有合适的安全保护措施。

（二）管理因素

管理因素主要是指网络管理漏洞。一般来说，在设计计算机网络系统的时侯，相关的工作人员在落实内部结构设计时所关注的重点实际上是外部环境对系统造成的威胁，或者存在的一些安全性因素等，从而就会忽视系统内部所存在的安全漏洞，或者可承受的攻击程度等，以至于在整个系

统的内部缺乏网络审计及跟踪机制方面的应急策略。与此同时，网络管理员在日常工作过程中，并没有过多地重视系统日志这些信息内容。另外还存在一些比较普遍的问题，例如，某些网络管理人员的专业素质不高，整体管理措施并不是十分完善；某些网络用户的安全意识不强等，这些都会引起网络安全问题。

（三）人为因素

我们可以把网络安全问题看作人的问题，无论是技术人员还是管理人员，在面对计算机网络安全问题的时候都需要承担一部分责任。也就是说，基于人的行为，可以将网络安全问题归结为两种：其一是技术人员和管理人员在工作过程中出现的无心错误，其二是外部环境中人为的恶意攻击。

1. 无意识的人为失误

一般情况下，出现这一类型的网络安全问题会涉及以下几个方面的因素：其一是计算机系统结构本身或者内部的设置出现故障，其二是技术人员或者管理人员在操作上出现失误，其三是软件系统本身出现错误。如技术或者管理工作人员，在各自的工作中出现安全配置不恰当的情况下，就会造成整个系统的安全漏洞，同时，也会因为网络上用户自身缺乏安全意识，给计算机网络的安全带来威胁。

2. 有意识的人为攻击

这一类型的恶意攻击通常是外部环境中的人找到了计算机系统中存在的漏洞，进而利用这一安全漏洞对计算机系统进行恶意攻击。也会有一些攻击者直接对计算机系统设备进行物理上的破坏。例如，攻击者可以利用计算机网络中的安全漏洞，将病毒传播到系统中，致使主机瘫痪。

（四）薄弱的认证环节

通常情况下，人们接触得最多的网络认证是口令的形式，实质上口令认证具有一定的薄弱性。这是因为有很多途径和手段，可以轻易地破解口令认证。一般情况下攻击者会将加密的口令进行技术上的解密，从而窃取口令，也有一些攻击者会通过网络通信渠道的形式窃取口令。现阶段无论是 TCP（transmission control protocol）服务还是 UDP（user datagram protocol）服务，在正常的认证工作中，主要针对的目标就是主机地址，很多时候基本上不能实现针对用户的指定认证。基于这样的特性，同一个服务器上的管理员只能够信任某一个主机上的某一个特定用户，并且管理员需要授权给该用户对系统的访问权。

（五）系统的易被监视性

一般情况下，用户使用 Telnet 或 FTP（file transfer protocol）实现远程主机上账户的链接。如果这一过程中传输的口令不进行加密处理，攻击者就可以对其操作进行监视，然后截获用户的账号及口令，在获得之后，通过正常的渠道就可以登录到系统中。如果入侵者在这一过程中截获的账号和口令是管理员的，那么在登录系统之后，入侵者的访问级别和权限就会更高，访问也会更容易。

（六）易欺骗性

正常情况下，主机的地址会得到 TCP 服务的信任，也会得到 UDP 服务的信任，攻击者如果使用的是 IP Source Routing，他可以通过以下几个步骤，把自己假扮成被信任的某一服务器中的客户。

步骤一：攻击者需要将自己的 IP（internet protocol）地址转换为某一服务器中被信任的客户的 IP 地址。

步骤二：攻击者需要构建出一条路径，这条路径涵盖被攻击的服务器，也涵盖其他的主机，其中需要把某一服务器中被信任的客户作为通向其他主机服务器路径上的一个重要结点。

步骤三：当路径建成之后，攻击者需要以被信任客户的身份发出申请。

步骤四：一旦服务器接受客户的申请，就如同这名被信任的客户本身发出的申请一样，系统就会对这一申请做出相应的反应。

步骤五：攻击者可利用系统中给出的反应路径对路径中的主机进行攻击和入侵。

一般情况下，诸多 UNIX 主机会在接收到这样的申请后，将入侵者的数据包继续在路径上进行传输，最终会传输到入侵者指定的位置。

（七）有缺陷的局域网服务和相互信任的主机

与其他设备的管理相比，主机方面的安全管理存在一定的困难，而且在管理上需要花费很多的时间，所以在管理工作过程中，工作人员会降低管理要求。管理过程中会在一些站点增加 NIS（network information service）和 NFS（network file system）服务，这类服务能够以数据库为路径，体现出分布式管理的优势，并且在管理过程中可以实现文件的共享和信息数据的共享。对于管理主机的工作人员来说，能够在很大程度上减轻他们的工作总量。可是这样的管理形式和服务类型，也存在着一些不安全的因素，对于一些有经验的

入侵人员来说，他们还是可以在这条路径上获得访问的权限。若是在主机的管理工作中，某一个中央服务器受到了攻击，会影响与它同时链接在一个路径上的其他系统，以至于中央服务器及整体系统都会受到不同程度的损害。

（八）复杂的设置和控制

主机系统的另外一个特征就是访问控制的配置难以验证，而且其配置结构异常复杂，所以入侵者可以利用偶然出现的配置错误来获取访问的权限。综上所述，计算机网络中很大一部分安全事故，之所以会出现，是因为入侵者能够发现在网络路径上存在的诸多薄弱点。从目前主机系统的结构来看，大部分的 UNIX 系统是以 BSD（berkeley software distribution，伯克利软件套件）为主体从网络上获得的源代码，但获得 BSD 的源代码的难度不大，这就让入侵者能够利用这条路径上的缺陷或者是薄弱点来制造入侵主机系统的机会。计算机网络安全之所以会存在缺陷和薄弱点，是因为软件系统本身的结构非常复杂，不能在测试的过程中保证对于每一种环境都是安全的。

（九）无法估计主机的安全性

时至今日，对于计算机主机系统整体的安全性，依旧没有一个科学合理的方法能对其进行完整的评估。现阶段主机的数量在增加，路径中的站点也在增加，以至于在中央系统中无法保证每一台主机均处在安全级别较高的位置上。对比某一个系统的管理和中央系统的管理，在管理中央系统时比较容易出错，另外的一个因素就是，主机系统的管理决策一直在发生变化，而且在运行上是比较缓慢的，这就会让一部分系统的安全性要低于另一部分系统的安全性，而这些安全性比较低的系统就会致使整体的中央系统遭到破坏。

二、网络攻击类型

计算机网络的主要功能是传输信息，信息传输主要面临的威胁包括如下四类：一是截获，即攻击者在网络路径上，通过窃取别人的信息资源和通信内容来获得传输的信息；二是中断，即攻击者在用户通信的路径上，有意识地中断别人的行为；三是篡改，即攻击者在用户网络传输的路径上有意识地篡改用户传输的报文；四是伪造，即攻击者在用户使用的网络传输路径上伪造用户原有的传输信息。

当前网络安全的威胁主要体现在以下几个方面：① 网络协议中的缺陷，如 TCP/IP 协议栈的安全问题等；② 窃取信息，如通过物理搭线、监视信息流、接收辐射信号、会话劫持、冒名顶替等形式窃取通信信息；③ 非法访