JISUANJI WANGLUO ANQUAN JISHU YANJIU

计算机网络安全技术研究

孟祥丰 白永祥 著

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

渭南师范学院出版专项经费资助项目

计算机网络安全技术研究

孟祥丰　白永祥　著

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

内容简介

本书以保障计算机网络的安全特性为主线，讲述实现计算机网络安全的数据保密性、数据完整性、用户不可抵赖性、用户身份可鉴别性、网络访问的可控性和网络可用性六大机制，系统地介绍了网络安全知识、安全技术及其应用，重点介绍了网络系统的安全运行和网络信息的安全保护，内容包括网络安全概论、网络安全系统模型、网络安全态势感知体系框架和态势理解技术、认证 Agent 的实现及防护、入侵检测技术方法、基于模型的网络安全风险评估、基于多目标攻击图的层次化网络安全解析、基于无线局域网的异构无线网络攻击环境及防御以及网络信息系统安全的技术对策。

图书在版编目(CIP)数据

计算机网络安全技术研究/孟祥丰，白永祥著．—北京：北京理工大学出版社，2013.10
ISBN 978-7-5640-8340-3

Ⅰ.①计…　Ⅱ.①孟…②白…　Ⅲ.①计算机网络-安全技术-研究　Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2013)第 217741 号

出版发行 /北京理工大学出版社有限责任公司
社　　址 /北京市海淀区中关村南大街 5 号
邮　　编 /100081
电　　话 /(010)68914775(总编室)
　　82562903(教材售后服务热线)
　　68948351(其他图书服务热线)
网　　址 /http://www.bitpress.com.cn
经　　销 /全国各地新华书店
印　　刷 /三河市天利华印刷装订有限公司
开　　本 /787 毫米×1092 毫米　1/16
印　　张 /10.25
字　　数 /264 千字
版　　次 /2013 年 10 月第 1 版　2013 年 10 月第 1 次印刷
定　　价 /46.00 元

责任编辑 /申玉琴
文案编辑 /申玉琴
责任校对 /周瑞红
责任印制 /马振武

前言

随着网络技术的飞速发展，网络安全问题变得日益严重，对网络安全的研究也越来越重要。目前，网络安全问题在许多国家已经引起了普遍关注，成为当今网络技术的一个重要研究课题。在网络安全领域，有很多网络安全技术，如防火墙、入侵检测、安全扫描、网络嗅探、协议分析、流量统计、网络管理以及蜜罐技术等。从技术上讲，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。

影响计算机网络安全的因素很多，除了信息的不安全性以外，层出不穷的电脑病毒也给网络安全带来了威胁。另外，黑客对于网络安全的威胁则日趋严重。网络所面临的威胁很多，其中包括：物理威胁（偷窃、废物搜寻、间谍行为、身份识别错误）、系统漏洞（乘虚而入、不安全服务、配置和初始化）、身份鉴别威胁（口令圈套、口令破解、算法考虑不周、编辑口令）、线缆连接威胁（窃听、拨号进入、冒名顶替）、有害程序（病毒、代码炸弹、特洛伊木马）。

当然，网络安全不仅是一个技术问题，也是一个社会问题和法律问题。要解决信息网络的安全问题，必须采取技术和立法等多种手段进行综合治理。

本书作为计算机网络安全技术研究的专著，采用通俗易懂的语言，围绕网络所涉及的安全问题，讲述了各种相关的安全技术，各章内容如下：

第一章是网络安全概论，包括网络安全简介、网络安全面临的威胁、网络出现安全威胁的原因、网络的安全机制。

第二章介绍网络安全系统模型。本章在仔细分析和研究了现有计算机系统模型、系统内核构建技术和安全操作系统的构建技术后，针对网络安全系统的特殊需求，提出一种不同于现有通用计算机系统模型的全新的网络安全设备的内核安全模型。

第三章介绍网络安全态势感知体系框架和态势理解技术。本章综合分析了网络的安全要素，评估了网络的安全状况，预测了其变化趋势，以可视化的方式展现给用户，并给出相应的应对措施和报表。

第四章介绍认证 Agent 的实现及防护。本章讨论认证 Agent 利用软件防火墙技术实现认证系统中的认证者以及粗粒度的网络访问控制，利用 SPI 会话层 DLL 中的 API 实现细粒度的网络访问控制。

第五章介绍入侵检测技术方法。本章主要分析现有主要入侵检测方法，并介绍入侵检测系统的分类，以及当前入侵检测所面临的问题和对检测系统性能的评估。

第六章介绍基于模型的网络安全风险评估。本章从评估标准、评估理论与方法、评估工具三个方面探讨了国内外信息安全风险评估领域的研究现状与进展，以及网络安全风险评估所面临的问题。

第七章介绍基于多目标攻击图的层次化网络安全解析。本章首先对网络安全特征进行了分析；然后提出了网络安全风险的概念模型；最后，提出了多目标攻击图来揭示目标网络内潜在威胁的传播路径。

第八章介绍基于无线局域网的异构无线网络攻击环境及防御。本章主要结合 WLAN 网络的安全威胁，针对 WLAN 和 3GPP 互联的松耦合方式下的认证协议进行分析和攻击防御。

第九章介绍网络信息系统安全的技术对策。

本书第一章、第二章、第四章、第五章、第六章、第八章、第九章由孟祥丰撰写；第三章、第七章由白永祥撰写；本书由孟祥丰统稿。

本书在撰写过程中，参考了大量书籍，在此对各部书的编著者表示感谢。在本书的撰写过程中，得到了很多朋友的帮助，在此对他们表示真挚的感谢。同时也感谢我的亲人，他们的支持和理解是我创作的动力。最后，我非常感谢渭南师范学院出版专项基金对本书出版的大力支持。

由于作者水平有限，再加上网络安全技术的发展十分迅速，书中难免有不妥和错误之处，恳请广大读者赐教。

作　者

目　录

第一章

概　论

随着计算机技术的迅猛发展和网络应用的日益广泛，互联网在人们的生产生活中扮演着越来越重要的角色。与此同时，黑客攻击、病毒木马、僵尸网络等各种网络安全事件也越来越多，严重威胁互联网的应用和发展。随着信息技术的发展和 Internet 技术的广泛应用，如今的网络已经成为人们生活中不可缺少的一部分，人们对信息网络系统的需求和依赖程度正在日益增加，与此同时，网络安全问题也变得非常严重。因此，分析影响网络安全的原因，提出保障网络安全的相关对策十分重要。本章正是围绕网络安全技术这一具有深刻技术背景和广泛应用前景的热点问题展开研究。

1.1　网络安全的基本概念

计算机网络安全是指计算机网络系统中的硬件、数据、程序等不会因为无意或恶意的原因而遭到破坏、篡改、泄露，防止非授权的使用或访问，系统能够保持服务的连续性，以及能够可靠地运行。它主要包括如下三个方面。

1. 物理安全

物理安全主要是指在物理介质层次上对存储和传输的网络信息的安全保护，防止计算机网络设备、设施遭受自然或人为的破坏。

2. 安全控制

安全控制是指在网络系统中对存储和传输信息的操作和进程进行控制和管理，在网络信息处理的层次上对信息进行安全保护。

3. 安全服务

安全服务是指在应用程序层次上对网络信息的保密性、完整性和真实性进行保护和鉴别，防范各种安全威胁和攻击。

其中，物理安全和安全控制是通过管理手段来保障计算机网络的安全性，而安全服务主要是从技术角度出发保证计算机网络的正常运行。

1.2　网络安全现状

1.2.1　严峻的网络安全形势

随着互联网的迅猛发展与网络应用的日益广泛与深入，网络成为影响各国政治、经济、军事、生活的一个重要因素。联合国发起的互联网管理论坛第二次会议在 2007 年 11 月 22 日公布的统

计数据显示,最近10年来全球上网人数显著增加,网民总数已从1997年年底的7 000万人增加到2007年的12亿人[1]。在国内,Internet应用也正在掀起新的高潮。中国互联网络信息中心(CNNIC)在2008年1月发布的《第21次中国互联网络发展状况统计报告》中指出,截至2007年12月,中国已达到16%的互联网普及率,网民数已增至2.1亿人,跃居世界第二。可见,互联网上的信息资源日趋丰富,网络教育、网上银行、即时消息、在线交易、网络广告、网络新闻、网上视频、电子邮件、网络资讯服务和网络游戏等服务业务快速发展,互联网已经成为影响最广、增长最快和市场潜力最大的产业之一,并且正以超出人们想象的深度和广度迅速发展。

在互联网迅速普及并对人们生产生活产生越来越大影响的同时,各种黑客入侵、网络攻击、恶意代码、病毒木马、僵尸网络等网络安全事件也呈指数级增长,造成的危害和损失也越来越严重。2001年暴发的红色代码蠕虫病毒,在其传播的最初9小时内就感染了超过25万个计算机系统,造成的损失以每天2亿美元的速度增长,最终高达26亿美元。在国内,根据CNCERT/CC《2007年上半年网络安全工作报告》,2007年1月至6月间,我国大陆地区被植入木马的主机IP远远超过2006年全年,增幅达21倍;被篡改网站数量比2006年同期增加了4倍;监测到感染僵尸网络的主机总数达520多万。国家计算机病毒应急处理中心和计算机病毒防治产品检验中心联合发布的《2007年中国计算机病毒疫情调查技术分析报告》指出,自2006年11月至今,我国连续出现"熊猫烧香""仇英""艾妮"等盗取网上用户密码账号的病毒和木马。病毒制造者、传播者追求经济利益的目的越来越强,利用病毒木马技术进行网络盗窃、诈骗活动,通过网络贩卖病毒、木马,传授病毒编制技术和网络攻击技术等形式的网络犯罪活动明显增多,严重威胁我国互联网的应用和发展,制约了网络银行等的普及应用,网上治安形势非常严峻。

1.2.2 网络安全监控

在这样的背景下,网络安全监控、网络安全预警及应急处理等得到了世界各国的普遍重视。从公开文献来看,美国、日本和中国等国家已建立了国家级网络安全事件监控系统。其中,美国从2001年开始计划研制全球预警信息系统GEWIS,对互联网的各种运行状态进行监控,并对一些可能发生的威胁,如对域名服务器(DNS)发起的DDOS攻击、蠕虫或病毒的大规模暴发等迹象进行监测并提前预警。日本约从2003年开始部署了互联网扫描数据获取系统ISDAS,通过分布在各地的传感器,获取各种如系统脆弱性、蠕虫感染、扫描行为等信息,对这些数据进行分析后,定期在官方网站上将各种安全态势进行发布、预警等。我国从2002年10月开始研发部署了"863-917"网络安全监测平台。该平台目前仍处于不断建设过程中,已成为国家网络安全应急处理体系的核心技术系统,为国家网络安全应急处理提供决策依据。

简单地讲,网络监控就是通过分析从网络上获取的通信、安全事件等信息,实现对网络运行状态的监视,帮助网络管理人员了解目标网络的运行状况,发现目标网络存在的安全问题,达到对网络进行有效管理和控制的目的,保证网络(系统)资源使用过程中的机密性、完整性和可用性。

图1.1给出了一个基本的网络监控系统结构[2]。网络上分布的各种采集器、入侵检测系统、病毒检测系统、漏洞扫描器、防火墙、分布式探针系统等数据采集设备(系统)捕获原始的监控数据,并进行一定的处理,如基于规则的监控数据过滤和监控数据格式标准化等,然后将监控数据传输给数据分析模块。数据分析模块分为两部分:在线实时处理和离线深度分析。对实时性要求较高的用户查询处理请求,由在线实时处理模块根据最新数据的情况进行分析,并实时输出结果,可以在线回答一些用户最关心的问题,如当前感染蠕虫最严重的区域是哪个?哪些重点服务器的访

问请求数超过了阈值？哪些机器的漏洞多且频繁遭受攻击？等等。一些重要的监控数据还需要进行归档存储，以进行进一步的离线处理，如安全事件关联分析、挖掘发现新的攻击等。数据分析模块的输出，包括动态的实时分析结果和离线挖掘结果，根据需要传递给各个后续应用模块（如风险评估、控制防御等），为之提供支持和辅助决策，进而实现网络监控应用系统的各种不同功能。

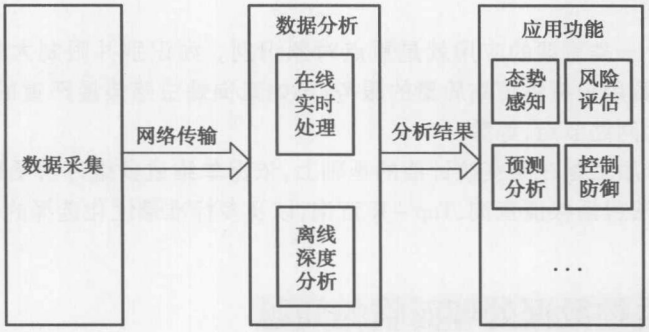

图 1.1　网络监控系统结构示意

数据分析是网络安全监控系统的关键功能模块之一。通过对数据进行多粒度、多角度的分析，可以发现网络安全事件，进而为后续的各种网络监控应用提供支持。下面通过对几个典型案例的简单分析，举例说明通过数据处理解决网络安全监控问题的应用。

1. 拒绝服务攻击监测

拒绝服务攻击通过向攻击目标发送大量的攻击数据包来消耗目标主机或网络的资源，达到剥夺计算机和网络提供正常服务能力的目标，是目前较常见的一类网络攻击行为。如在邮件炸弹攻击中，攻击者发送大量的 E－mail 到受害站点的一个或多个账号，试图消耗系统和网络的资源；TCP SYN Flood 攻击者通过发送大量包含不同源地址的 SYN 包[3]，使得接收者耗尽所有的链路资源，不能为合法用户提供服务，等等。

可以通过对主机网络的流量和连接特征进行分析，达到检测 DOS 攻击的目的。例如按照保护对象的 IP 地址，监测单位时间内进入网络的 SMTP 流量总和或链接总数，并与历史记录、系统设计规模或预设阈值等进行比较判断，就可以检测上述邮件炸弹和 TCP SYN Flood 攻击是否发生。涉及的数据处理操作包括 SUM、COUNT 以及阈值判断等。

2. 蠕虫

网络蠕虫[4]是一种具有巨大破坏力的恶意代码。它具有主动搜索扫描、自我复制等特性，无须用户干预便能够独立地进行主动攻击，因此具有更强的隐蔽性和破坏性。目前出现的如红色代码、Slammer2 等蠕虫都可以在很短的时间内主动攻击网络上具有相应漏洞的大量主机，给人们带来了巨大的损失。

对于已知的蠕虫，可以根据其特定的传播方式和有效载荷进行识别，如 Slammer worm 使用 376 字节的 UDP 包，发送到 1434 端口。对于未知的蠕虫，可以通过监控其自我复制和传播过程中，在网络包中出现超过期望值的相似字符串来进行发现。因此，对于已知蠕虫的监测、规模判断以及未知蠕虫的识别，可以结合监控数据上的 SUM、COUNT、Threshold、频繁项等查询处理来完成。

3. 垃圾邮件

垃圾邮件一般是指未经请求而发来的电子邮件，通常包含一些商业广告以及其他不良信息。垃圾邮件制造者用一个或多个邮件地址，在短时间内向外发送大量内容相同的邮件，因此会占用带宽、存储和运算资源，影响网络的正常运行；对于用户来说，处理垃圾邮件不但造成时间和费用

的浪费，而且有可能收到对系统安全构成威胁的病毒邮件。

可以按照源 IP 地址监测发出的 SMTP 流量来发现垃圾邮件制造者；另外，相同内容的垃圾邮件在短时间内频繁发送，因此可以通过频繁项监测来识别。涉及的数据处理包括 SUM、COUNT、Threshold 以及 Frequent Items 等。

4. 重点对象识别

网络监控中另外一类重要的应用就是重点对象识别。如识别并限制大量占用网络资源的用户，从而为其他大多数用户提供更高质量的服务；再如查询蠕虫感染最严重的局域网络，系统漏洞多且遭受攻击频繁的网络节点，等等。

重点对象识别本质上是在某些统计值的基础上，依据单维或多维评价函数进行最优化选择的问题，典型的处理方法包括极值查询、Top－K 查询，以及多标准最优化选择的轮廓查询处理等[5]。

1.2.3 网络监控数据处理面临的问题

在国家骨干网或大规模特定域网络上进行以网络安全为目的的监控，具有很多特性，这些特性使得网络监控数据处理面临着新的挑战。

1. 网络安全监控应用的特点

(1)数据规模大，产生速度快。在网络规模不断扩大、网民数量逐渐增多的背景下，国家骨干网和特定域大规模网络监控中产生的数据，越来越呈现海量性的特点。例如电信等服务提供商，管理着主干网络，通过高速交换机连接，其数据流速可达 40Gb/s。在这样高速的网络中进行监控，监控数据本身产生速度非常快，规模也会非常大。

(2)数据产生和监控任务的连续性。网络监控需要不间断持续进行，因此监控数据的产生也是连续的、无限的；监控查询的目的是根据最新监控数据及时跟踪最新结果，所以查询不是一次性的而是需要持续一段时间，查询结果本身会随着最新监控数据的到来而不断发生变化。

(3)对结果的实时性要求高。随着计算机相关技术的发展，黑客攻击方法和病毒技术也不断进步，破坏力越来越强，攻击速度也越来越快，在很短时间内就会造成巨大的损失。因此，网络安全监控数据处理的实时性要求越来越高。

(4)结果的近似性要求。在网络安全监控应用中，很多时候用户并不一定需要得到精确的查询结果，而仅需要一个满足精度约束的近似结果。例如网络路由器通过实时监控各个 IP 地址发送的数据包数量，可以检测是否有 DOS 攻击。对查询结果来说，IP 包数目到底是 50 175 还是 50 000 ± 1 000，差别并不大。如果计算精确结果需要耗费较长的时间，而仅需很短的时间便可计算出满足一定精度误差的近似结果，用户更青睐后者。

(5)仅关注异常。在网络安全监控中，监控的目的不是为了实时记录网络运行状态，更关注的是发现异常情况并及时进行处理，因此绝大部分监控仅对异常(非典型的)情况感兴趣，而正常行为则可以忽略。例如在基于阈值的 DOS 攻击检测中，用户希望随时发现远程连接数超过预设阈值的对象，并希望得到对应的近似连接数值；但是当对象的连接数低于阈值时，用户只需知道其处于正常范围即可，并不关心这些对象的具体连接值是多少；再如对僵尸网络的监控中，用户希望把注意力放在那些已经具备了一定规模的僵尸网络上(如包含节点数大于 1 000)，而小规模僵尸网络由于其危害性有限，可以暂时不去关注。

2. 网络安全监控数据处理面临的挑战

(1)海量、持续、快速到达的数据与有限的计算存储资源之间的矛盾。网络监控产生了海量的

监控数据。如何采用高效的方法对这些数据进行管理、分析，进而通过有限的计算存储资源处理无限快速到达的数据，是网络监控数据处理面临的首要挑战。

(2)分布的本质特性与网络带宽资源之间的矛盾。带宽资源是互联网上最紧张的资源之一。在网络监控系统中，数据采集设备部署在物理上分布的骨干路由等各种核心设施上，因此网络监控本质上是分布的。监控本身产生大量的数据，需要持续传递给集中式处理节点进行处理。由于监控数据与正常的网络流量负荷在同一网络中传输，所以监控系统会进一步加剧网络带宽资源的紧张情况。显然，如果把所有监控信息都传送到集中节点，会引起庞大的网络开销；定期取样(快照)的方法一方面会引起网络流量的周期性突发振荡，同时仍需考虑取样频率与通信开销的平衡：如果取样频率过高仍会导致较大的网络开销；如果取样频率过低会导致事件监测的延迟甚至丢失。因此，网络监控取样频率与网络带宽资源之间存在矛盾，如何在保证精度和事件监测实时性的前提下，降低监控引起的通信开销，成为网络安全监控数据处理面临的第二个挑战性问题。

(3)连续跟踪查询、实时得到近似结果的应用需求对数据处理技术提出了新的要求。网络监控需要对不断产生的监控数据进行处理，持续跟踪查询结果。该应用场景与传统的数据库、数据仓库等的应用场景存在较大差别。如果采用已有方法进行处理，在资源开销、执行效率、结果实时性等方面都存在一定问题。

1.3　网络安全问题的原因

1. 网络安全的内容

一般而言，网络安全包括以下6方面的内容。

(1)保密性(防止系统内信息非法泄露)。

(2)完整性(防止软件、程序与数据被非法删改和破坏)。

(3)可靠性(确保信道、消息源、发信人的真实性以及核对信息获取者的合法性)。

(4)合法性(保证信息及信息系统确实为授权使用者所用)。

(5)可控性(对信息及信息系统实施安全监控管理)。

(6)不可否认性(保证行为人不能否认自己的行为)。

2. 导致安全问题的主要原因

首先，系统软件，包括操作系统的结构和功能，正变得越来越复杂。使得软件设计者在设计时无法预料程序运行时的系统状态，更无法精确预测在不同的系统状态下会发生什么结果，所以系统漏洞的存在是在所难免的。

其次，随着互联网需求的日益增长，将来自系统外部的请求完全隔离是不可能的。系统的安全漏洞和系统的加密措施已不再像以前那样仅有为数不多的专业人士知道。在互联网上，有数以万计的黑客站点在时时刻刻地发布这些信息，并提供各种工具和技术以利用这些漏洞来破解保密体系，进行系统攻击。

最后，组成计算机网络的某些关键技术也并非绝对安全。如广泛应用的TCP/IP协议本身就有许多不完善之处。图1.2列举出了OSI七层标准中常见的一些漏洞[6]。

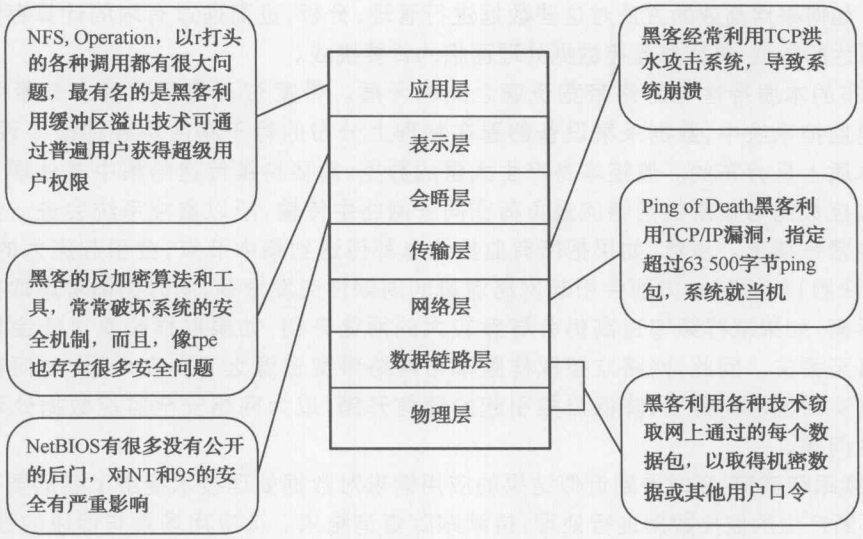

图 1.2　OSI 七层结构常见漏洞

1.4　解决网络安全问题的现有措施

为了防御种种攻击，目前采取了许多手段。信息的安全性管理其实是一种风险管理，因为在一个人为创造的网络交流环境中，不存在绝对安全，信息安全的实现也只是一个相对的概念，主要包括技术和非技术两方面的措施。

1.4.1　非技术措施

(1) 对系统使用人员加强安全意识教育。

(2) 制定安全策略。

(3) 加强对网络不法行为的制约。

1.4.2　技术措施

1. 认证技术

这种技术可以通过对机密信息，例如口令、个人身份号码加密密钥的确认来认证用户、网络主机以及文档的合法性，也可以使用智能卡、访问令牌或加密卡的方式，或者采用指纹识别、虹膜等生物测定法。这些方法都是行之有效的方法，但也不能排除在某些环境下出现意外的情况。例如，机密信息被破解、令牌被盗、生物测定法识别错误等。而且在认证技术中，存在一个最大的安全隐患，就是安全控制点，一旦攻击者攻破了安全控制点，那么所有采用的认证技术将形同虚设。

2. 密码术

密码术的用途有多种，它可以提供可信性保护、数据完整性认证、用户、主机和消息认证以及数字签名的功能，从而对开放网络环境下通信双方的通信内容和存储在主机上的文件数据提供保

护。密码术本身具有的特性，使它既可以作为一个系统形成一个独立的产品，也可以集成在其他应用程序或网络服务中，对用户透明。密码术本身的安全问题需要从加密算法、加密协议、密钥生成以及密钥管理这几个方面来考虑。

3. 访问控制

访问控制技术基于安全策略来控制用户对各类资源（如网络、计算机、应用程序以及各类信息）的访问。安全策略的制定可以根据使用者特定的需要，如针对独立的用户、集团，或根据访问时间、地点等。根据安全策略，访问控制需要对试图访问资源的用户进行身份认证。安全策略的制定和实现是访问控制能否成为“安全门卫”[7]的关键。

4. 审计技术

它记载了系统各级使用者与安全相关的各类活动。例如，成功或者不成功的登录、执行了哪些系统命令、运行了哪些应用程序、访问了哪些文件。审计功能的实现有自身的灵活性，既可以实现在系统级也可以实现在应用级。但是它同样有自身的弱点，一旦遭到篡改或删除，入侵者的行踪将无迹可寻。

5. 防火墙技术

一般将需要提供保护的局域网称为内部网。防火墙是隔离内部网和外部网的关口，它通过在内部网和外部网之间架构一个安全防护区，过滤内部网和外部网之间的通信，实现对内部网的安全保护。防火墙技术是计算机软件和硬件的综合实现，通过设定安全规则，防火墙决定是否让每个报文通过。安全规则的制定是防火墙技术的关键，安全规则的制定可以针对协议、源地址、目的地址或者端口号，以及通信内容（通常通过关键字的匹配实现）。防火墙技术是一种综合性很强的技术，它可以综合身份认证、加密技术和访问控制技术以及支持多种现有的安全通信协议来达到更高的安全性。但是防火墙技术同样有自己的弱点：首先，经伪装通过了防火墙的入侵者将在内部网上横行无阻；其次防火墙对于来自内部的攻击则束手无策；最后防火墙的技术缺乏系统性，尽管防火墙技术综合采用了多种计算机网络安全技术，它们分别在不同的层次上不同程度地解决了不同方面的网络安全问题，但是从来没有一个统一的体系或者标准把它们结合起来。由于不同的安全技术保护的对象是计算机网络的不同方面，所以每一种技术保护的范围都是有限的，然而网络面临的攻击却是多种多样的，防火墙技术无法完全抵御各种攻击。从另一方面来讲，采用了多种安全手段会导致配置、管理和使用上的复杂，太多的检测还可能导致网络性能的下降。

6. 入侵检测技术

入侵检测系统 DIS 的目的是检测出系统中的入侵行为以及未被授权许可的行为。入侵检测系统通过定时检查审计信息、监督网络流量来查找系统中当前发生的可疑事件。入侵检测系统和防火墙相结合，可以大大地扩展防御纵深，更好地保障网络的安全。

7. 反病毒技术

反病毒技术包括：病毒扫描，用以查找特定格式的病毒；杀病毒，用来清除病毒；完整性检验，用来检查病毒对文件和代码的修改和破坏。对于未知类型的病毒，反病毒技术还有待提高。

8. 系统脆弱性评估

真正成熟的安全技术需要做到“预防在前”。使用系统脆弱性评估工具对系统进行定期的脆弱点测试，是达到事前“预防”的手段之一。常用的评估工具有：密码破译器、密钥破解器、诊断程序、网络扫描器等。值得注意的是，很多黑客工具就可以用来当作系统脆弱性评估工具。

9. 可靠系统设计

要实现一个高可靠性的安全系统，首先需要有好的设计方案，而且安全通常是一个整体概念，

一个安全的系统不能仅仅依靠个别软件来实现，它既需要安全的上层应用软件，也需要有底层程序的支持。随着安全概念的扩展，一个可靠的系统不仅包括软件安全，还包括硬件安全以及系统框架安全。如果在实现一个系统之前，能够对种种安全因素进行周密的考虑，在设计上加以注意，将会大大提高所要实现系统的安全性和可靠性。

1.5 计算机网络安全评估

1.5.1 网络安全的基本要求

1. 机密性

机密性是指网络中的数据、程序等信息不会泄露给非授权的用户或实体。即信息只能够被授权的用户所使用，这也是一般人们所理解的安全概念。网络系统必须能够防止信息的非授权访问或泄露。

2. 完整性

完整性是指不因人为的因素而改变网络信息原有的内容、形式和流向，即不能被未授权的第三方修改。

3. 可用性

可用性是指网络中的信息可以被授权用户或实体访问，并且可以根据需要被使用的特性。即网络信息服务在需要时，准许授权用户或实体的使用，或者当网络部分受到破坏需要降级使用时，仍可以为授权用户或实体提供有效的服务。

4. 可控性

可控性是指授权机构对网络信息的传播和内容具有控制能力的特性，可以保证对网络信息进行安全监控。

5. 不可抵赖性

不可抵赖性是指在网络系统的信息交互过程中，确认参与者身份的真实性，保证发送方无法对他发送的信息进行否认，并且可以通过数字取证、证据保全，使公证方可以方便地介入，通过法律来管理网络。

1.5.2 网络安全评估的定义

对一个组织来说，解决网络安全的首要问题就是明白网络系统目前与未来的风险所在，充分评估这些风险可能造成影响的程度，做到对症下药，这就是网络安全评估。信息系统安全评估做出如下定义："依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。"

近年来，一些研究学者也根据自身理解给出了关于网络安全评估的定义。

张涛博士认为，网络系统的安全评估主要是指针对网络系统面临的脆弱性和各种威胁，确定