卓越系列

高等学校计算机基础教育课程“十二五”规划教材

信息安全技术

宋　红　主编　　吴建军　岳俊梅　副主编

“十一五”国家级规划教材的延续

系统阐述最新的信息安全技术知识

理论以够用为度，以实践应用为基础

大量操作系统、数据、网络安全的案例

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

高等学校计算机基础教育课程“十二五”规划教材·卓越系列

信息安全技术

主　编　宋　红

副主编　吴建军　岳俊梅

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

信息安全主要包括实体及硬件的安全、操作系统的安全、数据的安全、网络和移动通信安全4部分。其中，网络和移动通信安全是当前备受关注的问题。本书从信息安全的基础理论、计算机实体及硬件安全、密码技术、数据与数据库安全技术、操作系统安全与策略、计算机病毒及防范、网络安全技术、无线局域网安全、移动通信安全、黑客的攻击与防范技术等几方面来组织编写。

本书在作者总结多年教学经验的基础上，本着“理论知识以够用为度，重在实践应用”的原则进行编写，书中提供了大量的操作系统安全、数据安全、网络安全等方面的操作实例，帮助读者掌握信息安全技术的基本方法，并使之胜任信息安全及网络安全的管理工作。

本书适合作为应用型本科及高职高专计算机类专业及相近专业的教材，也可作为计算机网络管理员、信息安全管理员的培训教材或自学参考书。

图书在版编目（CIP）数据

信息安全技术/宋红主编. —北京：中国铁道出版社，2013.12

高等学校计算机基础教育课程“十二五”规划教材·卓越系列

ISBN 978-7-113-17656-3

Ⅰ. ①信… Ⅱ. ①宋… Ⅲ. ①信息安全－安全技术－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字（2013）第269685号

书　　名：信息安全技术
作　　者：宋　红　主编

策　　划：刘丽丽　　**读者热线：400-668-0820**
责任编辑：周　欣　彭立辉
封面设计：刘　颖
封面制作：白　雪
责任印制：李　佳

出版发行：中国铁道出版社（100054，北京市西城区右安门西街8号）
网　　址：http://www.51eds.com
印　　刷：北京新魏印刷厂
版　　次：2013年12月第1版　　2013年12月第1次印刷
开　　本：787 mm×1 092 mm　1/16　　印张：14.75　　字数：370千
印　　数：3 000册
书　　号：ISBN 978-7-113-17656-3
定　　价：30.00元

前 言

FOREWORD

随着信息技术和互联网的发展，信息安全问题逐步成为各界关注和讨论的焦点。信息技术和网络技术已深入到社会的各个领域，人类对信息和计算机网络的依赖性越来越大。2013 年 6 月 6 日，美国的一个秘密监控项目 “棱镜计划（PRISM）”曝光。据美国中情局有关职员爆料：“棱镜”计划始于 2007 年，其中包括两个秘密监视项目，一是监视、监听民众电话的通话记录，二是监视民众的网络活动。消息一出，举世震惊，也再次引发了人们对信息安全的重视。2013 年 8 月 8 日，国务院印发《关于促进信息消费扩大内需的若干意见》，要求加快信息基础设施演进升级，增强信息产品供给能力，加强信息消费环境建设。普及信息安全知识已经成为保护我国信息和网络安全的头等大事。对应用型本科以及高职高专计算机类专业和相近专业的学生开设信息安全技术课程是十分必要的。

信息安全主要包括实体及硬件的安全、操作系统的安全、数据的安全、网络安全和移动通信安全 4 部分，其中网络安全和移动通信安全是当前备受关注的问题。本书从信息安全的基础理论、计算机实体及硬件安全、密码技术、数据与数据库安全技术、操作系统安全与策略、计算机病毒及防范、网络安全技术、无线局域网安全、移动通信安全、黑客的攻击与防范技术等几方面来组织编写。

本书本着“理论知识以够用为度，重在实践应用”的原则进行编写，书中提供了大量的操作系统安全、数据安全、网络安全等方面的操作实例，帮助读者掌握信息安全技术的基本方法，并使之胜任信息安全及网络安全的管理工作。

本书的教学内容大约需要 60 学时。

第 1 章主要阐述了研究信息安全的重要性，简要地介绍了信息安全面临的威胁、信息安全技术和信息安全法规；第 2 章具体介绍了实体安全技术；第 3 章介绍了密码技术，包括常用加密技术介绍，并介绍了加密软件实例——PGP；第 4 章介绍了数据与数据库安全技术；第 5 章讲述了操作系统的安全与策略；第 6 章简要介绍了计算机病毒及防范，重点讲述计算机病毒的检测、防范和清除，对典型的计算机病毒进行了分析；第 7 章为网络安全技术，介绍了防火墙技术、入侵检测系统和虚拟专用网络；第 8 章介绍了无线局域网安全；第 9 章简要介绍了移动通信安全，包括智能手机安全及防范对策等；第 10 章主要介绍了黑客的攻击与防范技术，同时列举了常见的黑客攻击方法以及如何防范黑客的攻击。

本书以通俗易懂的文字阐述了信息安全技术的基本理论和基本方法，力求做到内容新颖、概念清楚，具有较强的实用性和适用性。本书适合作为应用型本科、高职高专和成人高校计算机专业和相近专业的教材，也可作为计算机网络管理员、信息安全管理员的培训教材或自学参考书。

本书由宋红任主编，吴建军、岳俊梅任副主编。具体编写分工：宋红编写了第1章、第2章、第3章，吴建军编写了第7章、第8章、第9章、第10章，岳俊梅编写了第4章、第5章、第6章。宋红负责全书的统稿工作。

由于时间仓促，编者水平有限，书中难免有疏漏与不足之处，衷心期望读者给予批评指正。

编　者

2013年10月

CONTENTS

目 录

第1章 信息安全概论

2013年6月6日，英国《卫报》和美国《华盛顿邮报》报道了美国的一个秘密监控项目“棱镜计划（PRISM）”，该计划的正式名号为“US-984XN”。据美国中情局相关职员爆料：“棱镜”计划始于2007年，受到美国情报机构监控的主要有10类信息：电邮、即时消息、视频、照片、存储数据、语音聊天、文件传输、视频会议、登录时间和社交网络资料的细节等。其中包括两个秘密监视项目：一是监视、监听民众电话的通话记录，二是监视民众的网络活动。消息一出，举世震惊，再次引发了人们对信息安全的重视。

1.1 信息与信息系统

1.1.1 信息的概念

信息概念作为科学术语最早出现在哈特莱1928年撰写的《信息传输》一文中。20世纪40年代，信息的奠基人香农给出了信息的明确定义：他认为“信息是用来消除随机不确定性的东西”，并推导出了信息测度的数学公式。这一定义被人们看作是经典性定义并加以引用。控制论创始人维纳则认为“信息是人们在适应外部世界，并使这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容和名称”。而我国科学家钟义信对信息给出的定义是：“信息是事物运动的状态与方式，是事物的一种属性。”可见，至今为止，信息的概念仍然是仁者见仁智者见智。

一般情况下，信息是指人们所说的消息，或者是通信的内容，包括各种文字、指令、数据、信号、图形等。根据对信息的研究成果，科学的信息概念可以概括为：信息是对客观世界中各种事物的运动状态和变化的反映，是客观事物之间相互联系和相互作用的表征，表现的是客观事物运动状态和变化的实质内容。

1.1.2 信息的性质

广义地说，信息是指人类感官所能直接或间接感知的消息。信息已经成为人类的一种资源，研究信息的性质有利于人们对信息的开发和利用。

信息具有依附性、动态性、可处理性、共享性、可传递性、异步性、可转化性、可伪性等性质。

1. 依附性

信息本身既看不见又摸不着，人们能够看得见摸得着的只是信息载体，如语言、文字、纸张、图像、声波、电磁波、磁介质等，而非信息本身。信息只有依附于一定的载体，才能为人们所交流和共享。也正是因为有了这些载体，信息才变为一种广泛的资源与财富。

2．动态性

信息所反映的总是特定时刻事物运动的状态与方式，当该时刻的信息被提取出来后，事物仍在不停地运动。这样，已脱离于物质的信息就会渐渐失去效用，最终只能作为一种历史记录。信息的动态性也称之为信息的时效性，只有充分重视和发挥信息的时效性，才能将信息转化为时间和效益。例如，现在的金融信息，在需要知道的时候，会非常有价值，一旦过了这一时刻，信息就会毫无价值。又如，战争时的信息，敌方的信息在某一时刻具有非常重要的价值，可以决定战争或战役的胜负，但过了这一时刻，该信息就变得毫无用处。所以，相当部分的信息具有非常强的时效性。

3．可处理性

信息是事物运动的状态与方式，它可以依附于一切可能的物质载体。同样的信息可以用语言文字表达，也可以用声波来载荷，还可以用电流和光波来表示。但无论信息的载体如何变换，信息的内容都可以保持不变。信息的可处理性是通信技术和计算机技术发展的理论支撑点。

4．共享性

信息能够共享是信息不同于物质和能量的最重要的特征。萧伯纳对信息的共享性有一个形象的比喻：你有一个苹果，我有一个苹果， 彼此交换一下，我们仍然是各有一个苹果。如果你有一种思想，我也有一种思想，我们相互交流，我们就都有了两种思想，甚至更多。这个例子说明信息不会像物质一样因为共享而减少，反而可以因为共享而衍生出更多信息。信息的共享是人们应该努力追求的目标。

5．可传递性

信息传递的实质，就是一种事物运动的状态与方式脱离开源物质而附着于另一事物，并通过后者的运动将这种状态与方式在空间中从一点传到另一点。信息能够在时间和空间中传递，保证了它能够为人们所共享。

6．异步性

异步性是动态性的延伸，一般包括滞后性和超前性两个方面。信息脱离源物质后，需要经过输入、处理、传递、输出等过程才能为人们所理解和掌握，而此时源物质已发生新的变化，这些信息因而会成为“过时”的信息。另一方面，人们在掌握大量信息的基础上，又可以通过计划、预测等方式测知未来的信息，超前于现实，因而信息又具有超前性。

7．可转化性

信息在一定的条件下可以转化为物质、能量、时间、效益、质量、能力等。正确而有效地利用信息，可以在同样的条件下创造更多、更好的物质财富，可以开发或节约更多的能量，可以节省更多的时间与资金。

8．可伪性

信息的可伪性与信息的相对独立有关。一方面人们容易凭主观想象来认识和理解信息，从而易于产生虚假信息；另一方面人们容易孤立地认识和理解信息，从而易于产生片面的信息。此外，由于人们的认识能力有限或动机不纯，也容易形成伪信息。所以，一定要注重信息的来源和信息的鉴别，要有效防止信息污染。

1.1.3　信息的功能

信息的功能是信息属性的体现。信息的功能可分为两个层次，其基本功能在于维持和强化世界的有序性动态性，其社会功能则表现为维系社会的生存、促进人类文明的进步和自身的发展。

具体地讲，信息的功能主要表现在以下五方面：

① 信息是宇宙万物有序运行的内在依据。

② 信息是人类认识世界和改造世界的中介。

③ 信息是维系社会生存与发展的动因。

④ 信息是智慧的源泉，是人类的精神食粮。

⑤ 信息是管理的灵魂。

此外，信息还是一种重要的社会资源，是支持现代社会发展的重要支柱。人们生产和生活的质量将越来越多地取决于对知识信息的掌握和运用程度。

1.1.4　信息系统

信息系统是一个由人、计算机及其他外围设备等组成的能进行信息的收集、传递、存储、加工、维护和使用的系统。

信息系统不仅是一个技术系统，而且是一个社会系统。首先，信息系统的发展是伴随着计算机技术的发展而展开的，计算机技术是它得以存在的基础。计算机技术的发展直接推动了信息系统从低级低效发展到了高级高效。信息系统作为一个基于计算机的系统，其数据分析、软件开发等都需要技术的支持。同时，对于信息系统的开发和使用都需要专业的人来做，因此信息系统是一个技术系统。其次，信息系统是社会系统的抽象表达，社会系统的各个实体之间通过信息发生相互作用，而把这些实体抽象成为信息系统里的结点，将不可见的信息具体化，进行分类、检索和存储，提高信息的质量，就可以提高实体之间交流和相互作用的效率。任何一个实际有效的信息系统都是一个社会系统的映像，信息系统的运作可以提高社会系统的运作效率。它实际上也是社会系统的一部分，是社会系统高度发达的产物。

综上所述，对信息系统给出以下定义：信息系统是由计算机硬件、网络和通信设备、计算机软件、信息资源、信息用户和规章制度组成的以处理信息流为目的的人机一体化系统。

1.2　信息安全面临的威胁

1.2.1　信息安全的含义

信息安全起源于计算机安全，随着计算机网络技术的不断发展，单纯的计算机安全开始向信息安全演进。由于人们理解的形式不同，国内外对于“信息安全”并没有统一的定义。

国际标准化组织（ISO）的定义是指“信息网络的硬件、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，系统连续可靠正常地运行，信息服务不中断。”《中华人民共和国计算机系统安全保护条例》的定义为：“计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。”国家信息安全重点实验室对信息安全给出的定义是：“信息安全涉及信息的机密性、完整性、可用性、可控

性。综合来说，就是要保障电子信息的有效性。”

广义的信息安全是指网络系统的硬件、软件及其系统中的信息受到保护。信息安全有以下几个特点：

① 保密性：保护数据不受非法截获和未经授权浏览。它是信息安全一诞生就具有的特性，也是信息安全主要的研究内容之一。这点对于敏感数据的传输尤为重要，同时也是通信网络中处理用户的私人信息所必需的。存储信息的机密性主要通过访问控制来实现，不同的用户对不同的数据拥有不同的使用权限。通俗地讲，就是未授权的用户不能够获取敏感信息。对纸质文档信息，只需要保护好文件，不被非授权者接触即可。而对计算机及网络环境中的信息，不仅要制止非授权者对信息的阅读，也要阻止授权者将其访问的信息传递给非授权者，以致信息被泄露。

② 完整性：即保障被传输、接收或存储的数据是完整的、未被篡改的特性。完整性是保护信息保持原始的状态，使信息保持其真实性。这对于保证重要数据的精确尤为关键。如果信息被蓄意地修改、插入、删除等，形成虚假信息将带来严重的后果。除了数据本身不能破坏外，数据的完整性还要求数据的来源具有正确性和可信性。

③ 可控性：保证信息和信息系统的授权认证和监控管理，防止非法利用信息和信息系统。可确保某个实体(人或系统)身份的真实性，也可确保执政者对社会的执法管理行为。

④ 可用性：指对信息和信息系统实施安全监控管理，使授权主体在需要信息时能及时得到服务的能力。尽管存在可能的突发事件，如供电中断、自然灾害、事故或攻击等，但用户依然可得到或使用数据，服务也处于正常运转状态。当然，数据不可用也可能是由软件缺陷造成的。可用性是在信息安全保护阶段对信息安全提出的新要求，也是在网络化空间中必须满足的一项信息安全要求。

⑤ 不可否认性：能够保证信息行为人不能否认其信息行为。可防止参与某次通信交换的一方事后否认本次交换曾经发生过。数据签名技术是解决不可否认性的重要手段之一。

总体来看，信息安全就是要保证信息的基本属性不被破坏，信息按照发送方的意愿成功被接收方接收。

1.2.2 信息安全受到威胁的危害性

信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家安全战略。信息安全受到威胁的危害性无论对个人、企业、国家或者世界和平都是非常严重的。

据统计，2013 年二季度国内新出现木马病毒 5.27 亿个，1.57 亿网民遭遇攻击，约占国内计算机用户数量的 30%。有近 70%的企业用户处于“高度风险”级别，我国每年因网络泄密导致的经济损失高达上百亿。例如，2013 年上半年，一种名为比特币的新型虚拟货币在网上异常火爆，其兑换峰值曾高达 1 比特币兑换 266 美元。然而据业内人士透露，今年 3 月，一家比特币中介公司就曾遭到黑客攻击，被盗走价值 12 480 美元（约合 7.7 万元人民币）的比特币。由于比特币的特殊性，被盗后基本无法找回，所有损失只能由该中介公司自行承担。此外，针对留学生的 QQ 盗号和高额诈骗也频频发生，Cookie 也成为不法分子盗取用户隐私的重要途径，给人们的网络生活带来了巨大的风险。

随着移动互联技术的发展和普及，一些不法分子开始利用微博、微信等互联网社交平台的定位功能，定向追踪用户的隐私信息，给企业及个人造成巨大安全威胁。另外，近期多款国内外知名无线路由器也频繁被曝出存在漏洞，黑客可以通过该类漏洞对企业及个人用户进行长时间监控。

2013 年 6 月，斯诺登揭露了美国的“棱镜”项目，国家级信息战至此全面爆发。以前人们认为信息安全面临的威胁主要是信息泄露、拒绝服务和信息破坏，而事实上，维护信息内容安全才是当前最为紧迫的任务。目前全球共有 13 台根服务器，其中主根服务器 1 台，辅根服务器 12 台。主根服务器和 9 台辅根服务器分布在美国本土，另外 3 台分别在英国、瑞典和日本。这就是说，当前，美国持有互联网根服务器的控制权，这实际上就等于掌握了全球互联网的最终控制权。

对信息安全的威胁，按其严重性可分为三级：

① C 级威胁：指个体单点攻击。其攻击的范围、深度和能够完成的攻击任务不太复杂，往往是黑客行为，虽然这种攻击可以逐步实施自动化、平台化，但攻击点是一点，作用有限，通常攻击的是标准化网络和系统。

② B 级威胁：指有组织分布式协同攻击。多点、多技术和协同攻击，相互掩护，危害大，难于对付。其采用多种网络攻击技术，能够攻击一些专用网络和非标准网络，攻击软件本身并没有组织化，较少实施或不能实施战术。

③ A 级威胁：指通过一切手段，如可控计算机病毒、信息炸弹、远程攻击软件、网络攻击平台、使用多技术体制的网络、使用包括卫星通信在内的一切可利用的通信网络等，破坏对方信息系统的作战方式。例如，通过破解信息，为其所用；突破安全系统，破坏信息的真实和完整性；通过干扰阻止信息的传递；通过信息炸弹等手段使信息系统瘫痪。其本质就是一场信息战。

1.2.3　威胁信息安全的因素

安全威胁是指对安全的一种潜在的侵害。威胁的实施称为攻击。一般认为，目前信息安全面临的威胁主要表现为三类：信息泄露、信息破坏、拒绝服务。其中信息泄露、信息破坏也可能造成系统拒绝服务。

信息泄露指敏感数据在有意或无意中被泄露出去或丢失，它通常包括，信息在传输中丢失或泄露（如利用电磁泄漏或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析推出有用信息），信息在存储介质中丢失或泄露，通过建立隐蔽隧道等窃取敏感信息等。

信息破坏指以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加，修改数据，以干扰用户的正常使用。

拒绝服务指不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

安全威胁可能来自各个方面，归纳起来威胁信息安全的因素主要有以下 7 种：

① 自然及不可抗拒因素：指地震、火灾、水灾、风暴以及社会暴力或战争等，这些因素将直接地危害信息系统实体的安全。

② 硬件及物理因素：指系统硬件及环境的安全可靠，包括机房设施、计算机主体、存储系统、辅助设备、数据通信设施以及信息存储介质的安全性。

③ 电磁波因素：计算机系统及其控制的信息和数据传输通道，在工作过程中都会产生电磁波辐射，在一定地理范围内用无线电接收机很容易检测并接收到，这就有可能造成信息通过电磁辐射而泄露。另外，空间电磁波也可能对系统产生电磁干扰，影响系统正常运行。

④ 软件因素：软件被非法删改、复制与窃取将使系统的软件受到损失，并可能造成泄密。

计算机网络病毒也是以软件为载体侵入系统进行破坏的。

⑤ 数据因素：指数据信息在存储和传递过程中的安全性，这是计算机犯罪的主攻核心，是必须加以安全和保密的重点。

⑥ 人为及管理因素：涉及工作人员的素质、责任心，以及严密的行政管理制度和法律法规，以防范人为的主动因素直接对系统安全所造成的威胁。

⑦ 其他因素：指系统安全一旦出现问题，能将损失降到最小，把产生的影响限制在许可的范围内，保证迅速有效地恢复系统运行的一切因素。

1.3 信息安全技术

1.3.1 基本的信息安全技术

既然有威胁信息安全的因素存在，就应该有抵御这些威胁的措施。为了保证信息系统安全所采用的技术统称为信息安全技术。

随着信息安全的内涵不断延伸，信息安全也从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。目前，常用的信息安全技术主要有以下几种：

① 身份认证技术：用来确定用户或者设备身份的合法性，典型的手段有用户名、密码、身份识别、PKI 证书和生物认证等。

② 加解密技术：在传输过程或存储过程中进行信息数据的加密、解密，典型的加密体制可采用对称加密和非对称加密。

③ 边界防护技术：防止外部网络用户以非法手段进入内部网络，访问内部资源，保护内部网络操作环境的特殊网络互连设备，典型的设备有防火墙和入侵检测设备。

④ 访问控制技术：保证网络资源不被非法使用和访问。访问控制是网络安全防范和保护的主要核心策略，规定了主体对客体访问的限制，并在身份识别的基础上，根据身份对提出资源访问的请求加以权限控制。

⑤ 主机加固技术：操作系统或者数据库的实现会不可避免地出现某些漏洞，从而使信息网络系统遭受严重的威胁。主机加固技术对操作系统、数据库等进行漏洞加固和保护，提高系统的抗攻击能力。

⑥ 安全审计技术：包含日志审计和行为审计，通过日志审计协助管理员在受到攻击后查看网络日志，从而评估网络配置的合理性、安全策略的有效性，追溯分析安全攻击轨迹，并能为实时防御提供手段。通过对员工或用户的网络行为审计，确认行为的合规性，确保管理的安全。

⑦ 检测监控技术：对信息网络中的流量或应用内容进行检测并适度监管和控制，避免网络流量的滥用、垃圾信息和有害信息的传播。

1.3.2 信息安全防护思路

为了保证信息系统的安全性，降低信息系统所面临的安全风险，单一的安全技术是不够的。根据信息系统面临的不同安全威胁以及不同的防护重点和出发点，对应不同的网络安全防护方法。下面介绍一些有效的网络安全防护思路。

1．基于主动防御的边界安全控制

以内网应用系统保护为核心，在各层的网络边缘建立多级的安全边界，从而实施进行安全访问的控制，防止恶意的攻击和访问。这种防护方式更多的是通过在数据网络中部署防火墙、入侵检测、防病毒等产品来实现。

2．基于攻击检测的综合联动控制

所有的安全威胁都体现为攻击者的一些恶意网络行为，通过对网络攻击行为特征的检测，从而对攻击进行有效的识别；通过安全设备与网络设备的联动进行有效控制，从而防范攻击。这种方式主要是通过部署漏洞扫描、入侵检测等产品，并实现入侵检测产品和防火墙、路由器、交换机之间的联动控制。

3．基于源头控制的统一接入管理

绝大多数的攻击都是通过终端的恶意用户发起，通过对接入用户的有效认证，以及对终端的检查可以大大降低信息网络所面临的安全威胁。这种防护是通过部署桌面安全代理，并在网络端设置策略服务器，从而实现与交换机、网络宽带接入设备等联动实现安全控制。

4．基于安全融合的综合威胁管理

未来的大多数攻击将是混合型的攻击，某种功能单一的安全设备将无法有效地对这种攻击进行防御，快速变化的安全威胁形势促使综合性安全网关成为安全市场中增长最快的领域。这种防护通过部署融合防火墙、防病毒、入侵检测、VPN 等为一体的 UTM 设备来实现。

5．基于资产保护的闭环策略管理

信息安全的目标就是保护资产，信息安全的实质是“三分技术、七分管理”。在资产保护中，信息安全管理将成为重要的因素，制定安全策略、实施安全管理并辅以安全技术配合，从而形成对资产的闭环保护。目前，典型的实现方式是通过制定信息安全管理制度，同时采用内网安全管理产品以及其他安全监控审计等产品，从而实现技术支撑管理。

1.4　信息安全工程

1.4.1　信息安全工程概述

信息安全工程既不是纯粹的技术，也不是简单的安全产品的堆砌，而是一项复杂的系统工程。信息安全工程是采用工程的概念、原理、技术和方法来研究、开发、实施与维护企业级信息与网络系统安全的过程，它是将经过时间考验证明是正确的工程实施流程、管理技术和当前能够得到的最好的技术方法相结合的系统。

信息安全工程应该注意以下 5 个因素：

① 信息安全具有全面性。信息安全问题需要全面考虑，系统安全程度取决于系统最薄弱的环节。

② 信息安全具有过程性或生命周期性。

③ 信息安全具有动态性。安全技术在发展，黑客水平也在提高，安全策略、安全体系、安全技术也必须动态地调整，最大限度地使安全系统能够跟上实际情况的变化发挥效用，使整个安全系统处于不断更新、不断完善、不断进步的动态过程中。

④ 信息安全具有层次性。

⑤ 安全具有相对性。安全是相对的，没有绝对的安全。

1.4.2 信息安全工程的设计原则

信息安全系统的设计是一个周而复始、螺旋上升的过程。事实上，绝对的安全是不存在的，要做的是在保密性、可用性、完整性和成本之间取得最大限度的平衡。有这样一句话："七分管理、三分技术"，可见，安全保证的两大支柱是管理和技术，只有在管理方面明确思路，技术才有用武之地。

下面仅从技术角度给出信息安全系统的一些设计原则：

① 木桶原则：应坚持"木桶的最大容积取决于最短的一块木板"的原则，安全机制和安全服务设计的首要目的是防范最常用的攻击手段，因此应提高整个系统的"安全最低点"的安全性能。

② 整体性原则：应提供安全防护、监测和应急恢复，以便在网络被攻击、被破坏时，尽可能快地恢复网络信息中心的服务，减少损失。

③ 有效性与实用性原则：即如何在确保安全性的基础上，把安全处理的运算量减小或分摊，减少用户记忆、存储工作和安全服务器的存储量、计算量。

④ 安全性评价原则：即实用安全性与用户需求和应用环境紧密相关，根据不同的应用环境采取相应的安全措施

⑤ 动态化原则：即整个系统内尽可能引入更多的可变因素，并具有良好的扩展性。由于用户在不断增加，网络规模在不断扩大，网络技术本身的发展变化也很快，而安全措施是防范性的、持续不断的，所以制定的安全措施必须不断适应网络发展和环境的变化。

⑥ 设计为本原则：安全与保密方面的设计应与系统设计相结合，即在系统进行总体设计时考虑安全系统的设计，二者合二为一。

⑦ 有的放矢、各取所需原则：即在考虑安全问题解决方案时必须考虑性能价格的平衡，而且不同的系统所要求的安全侧重点各不相同，应把有限的经费花在刀刃上。

除以上原则外，再给出美国著名信息系统安全顾问 C.C.沃得提出的 23 条设计原则，以供参考。

① 成本效率原则：应使系统效率最高而成本最低，军事设施除外。

② 简易性原则：简单易行的控制比复杂的控制更有效、更可靠，而且受人欢迎、节省费用。

③ 超越控制原则：一旦控制失灵（紧急情况下）时，要采取预定的控制措施和方法步骤。

④ 公开设计与操作原则：保密并不是一种强有力的安全方式，过分信赖可能会导致控制失灵。对控制的公开设计和操作，反而会使信息保护得以增强。

⑤ 最小特权原则：只限于需要才给予这部分特权，但应限定其他系统特权。

⑥ 分工独立性原则：控制、负责设计、执行和操作的不应该是同一人。

⑦ 设置陷阱原则：在访问控制中设置一种易入的陷阱，以引诱某些人进行非法访问，然后将其抓获。

⑧ 环境控制原则：对于环境控制这一类的问题，应予以重视。

⑨ 接受能力原则：如果各种控制手段不能为用户或受这种控制影响的人所接受，控制则无法实现。因此，采用的控制措施应使用户能够接受。

⑩ 承受能力原则：应该把各种控制设计成可承受最大多数的威胁，同时也能承受那些很少遇到威胁的系统。