21世纪高等开放教育
系列教材

主　编｜蔡大鹏　康海燕
副主编｜姚大川

网络安全与管理

WANGLUO
ANQUAN　YU　GUANLI

中国人民大学出版社

系列教材

主　编 | 蔡大鹏　康海燕
副主编 | 姚大川

网络安全与管理

WANGLUO
ANQUAN YU GUANLI

中国人民大学出版社
• 北京 •

图书在版编目（CIP）数据

网络安全与管理 / 蔡大鹏，康海燕主编. —北京：中国人民大学出版社，2018.12
21世纪高等开放教育系列教材
ISBN 978-7-300-26366-3

Ⅰ. ①网… Ⅱ. ①蔡… ②康… Ⅲ. ①计算机网络-安全技术-高等学校-教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2018）第 236469 号

21世纪高等开放教育系列教材

网络安全与管理

主　编　蔡大鹏　康海燕
副主编　姚大川
Wangluo Anquan yu Guanli

出版发行	中国人民大学出版社		
社　　址	北京中关村大街 31 号	**邮政编码**	100080
电　　话	010-62511242（总编室）	010-62511770（质管部）	
	010-82501766（邮购部）	010-62514148（门市部）	
	010-62515195（发行公司）	010-62515275（盗版举报）	
网　　址	http://www.crup.com.cn		
	http://www.ttrnet.com（人大教研网）		
经　　销	新华书店		
印　　刷	北京宏伟双华印刷有限公司		
规　　格	185 mm × 260 mm　16 开本	**版　　次**	2018 年 12 月第 1 版
印　　张	9.75	**印　　次**	2018 年 12 月第 1 次印刷
字　　数	216 000	**定　　价**	28.00 元

前　言

随着科技的发展，互联网深入到经济社会的各个领域，网络安全正面临着严峻的挑战。网络安全就是网络上的信息安全，是指网络系统的硬件、软件和系统中的数据受到保护，不因偶然的或者恶意的攻击而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。2017 年 9 月，在北京召开了中国互联网安全大会，说明国家已经开始重视网络安全。在大会上，专家明确指出，网络安全不仅仅针对网络本身，而是包含社会安全、基础设施安全、人身安全等在内的“大安全”概念，迫切需要建立与之相适应的保障体系。

本教材选取了网络安全的主流技术、方法、管理手段等进行介绍，将带领读者更好地了解网络安全，了解网络安全给我们带来的影响，以及通过各种手段来防范各类网络安全威胁。

1. 内容结构

本教材共分为七个单元，第一单元是信息安全，主要讲述了信息与信息安全的概念、信息安全的实现、信息安全的发展与现状等；第二单元是计算机病毒，主要讲述了计算机病毒的概念、典型病毒和恶意软件的分析与清除等；第三单元是智能手机信息安全，主要讲述了智能手机信息安全、智能手机病毒、智能手机隐私泄露等；第四单元是网络安全技术，主要讲述了防火墙技术、入侵检测技术、VPN 技术等；第五单元是密码学基础，主要讲述了密码学的概念，以及古典密码、对称密码、非对称密码和认证技术等；第六单元是信息安全管理与法律法规，主要讲述了信息安全管理、信息安全法律法规、信息安全等级保护等；第七单元是黑客攻击技术，主要讲述了攻击的一般流程、攻击的方法与技术、网络后门与网络隐身等。

2. 本书特点

（1）知识新颖：在知识点的选择上，本教材不仅选取了基础的网络安全知识与技术，也选择了如今流行的网络安全技术以及各类网络安全问题，保证读者学习的知识不落伍。

（2）结构合理：本教材在每一单元都会提出问题等引导读者思考，并且总结知识点，易于读者了解并建立知识结构；从多角度讲解各知识点，使读者快速抓住重点。

编　者

目录 CONTENTS

CONTENTS

目录

第一单元

信息安全

Unit

学习导引

同学们好！欢迎你们来到“网络安全与管理”课程的课堂。这门课程将带领我们更好地了解信息安全，了解信息安全给我们带来的影响，以及通过各种手段来防范各类信息安全问题。首先，让我们查看一下自己的计算机，计算机里是否存有各类安全软件？你是否经常给计算机系统打补丁？计算机中是否有防火墙？这类软件是做什么用的？我们面临着哪些信息安全威胁？信息安全是如何发展的？请你们带着疑问，共同进入本单元的主题。

在本单元，我们将共同学习信息与信息安全、信息安全的需求与实现、信息安全的发展等内容。学完之后，相信你对信息安全会有一个全新的认识。

在本单元的学习之旅中，需要你们认真学习本单元的内容，观看教学视频，完成在线学习活动以及作业。只有按照要求完成上述所有环节的内容，你才算完成了本单元的学习任务。

学习目标

学完本单元内容之后，你将能够：

（1）掌握信息与信息安全的概念；

（2）了解信息安全的威胁、实现；

（3）了解信息安全的发展阶段，举例说明信息安全的发展现状。

接下来，让我们一步步深入理解本单元的学习内容吧。首先，我们来熟悉一下本单元内容的整体框架。

知识结构图

图 1－1 是本单元的整体框架以及学习这部分内容的思维过程规划。此图可以帮助大家从整体上了解本单元的知识结构和学习路径，包括信息安全概述、信息与信息安全、信息安全的实现、信息安全的发展与现状。请大家仔细品读和理解，建立对本部分知识的整体印象。

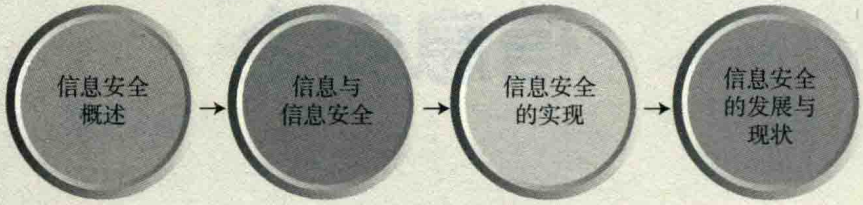

图 1－1　本单元知识结构图

看完上面的知识结构图后，大家是否已经对本单元所要学习的内容以及如何学习这些内容有一个初步的整体印象了呢？接下来，我们在这个整体框架的指引下逐一学习每个知识点。我们在了解了操作计算机时的疑问后，需要学习信息与信息安全的概念、特征等，着重学习信息安全的各种实现技术，以及信息安全的发展与现状。结合生活经验和对相关问题的认识，将理论与实践相结合。

知识点 1 信息安全概述

学前思考 1：

淘宝网上有店铺曾出售“58 同城简历数据”，一位淘宝店主表示：“一次购买 2 万份以上，3 毛钱一条；一次购买 10 万份以上，2 毛钱一条。要多少有多少，全国同步实时更新。”而其他店主则表示花 700 块钱买一套软件，就可以自己采集 58 同城的数据，有效期长达一个月。

为何我们的个人数据被泄露？为什么每个同学的计算机或者手机上都安装了各类杀毒软件？为什么要接受各种安全宣传，比如让我们不要随意下载软件，不要随意点击链接？

请你参考更多资料，思考一下，各种信息安全问题给我们带来了怎样的影响，我们应该如何防范。让我们带着问题学习以下内容吧。

本节知识重点

学习提示：各类安全问题一直困扰着我们，在本部分，我们可以发现信息安全的一些疑问，以及信息面临的威胁等。如果单纯阅读教材上的内容有障碍，我们可以通过观看视频《关于信息安全的一些疑问》来加深理解，然后完成在线学习活动 1。

一、一些疑问

在使用计算机的时候，我们经常会遇到一些安全疑问，比如：

（1）为什么我们要安装杀毒软件？现在市面上的杀毒软件这么多，国外的有诺顿、卡巴斯基、Mcafee 等，国内的有 360、金山、瑞星等，究竟哪一款杀毒软件查杀病毒的效果更好一些呢？

（2）我随意点击了浏览器的某个广告、某个链接，从未验证的网站下载软件或手机应用，有可能会发生什么事？

（3）我连接了一个免费 Wi-Fi，有可能会发生什么事？

（4）为什么我的 QQ 账号会被盗用？

（5）如果有一天，我发现自己的计算机运行很慢，怀疑计算机有病毒，那么应该怎样做应急处理呢？怎样找出病毒隐藏在什么地方呢？

（6）为何要为计算机安装补丁？不安装补丁会怎么样？

（7）我喜欢把密码设置成“123456”或者是我的生日日期，这样做对我的账号安全会有什么影响？

（8）防火墙是做什么的？如何使用软件防火墙来封锁一个 IP 地址或一个端口？

（9）当信息系统遭受攻击的时候，为什么经常会查到攻击人的 IP 地址在日本、美国甚至是欧洲的某些国家呢？难道真的有日本人、美国人或是欧洲人在攻击信息系统吗？

二、信息面临的威胁

信息的安全威胁是永远存在的，如图 1－2 所示，信息的安全威胁真是无处不在。下面从信息安全的五个层次来介绍信息安全中的威胁。

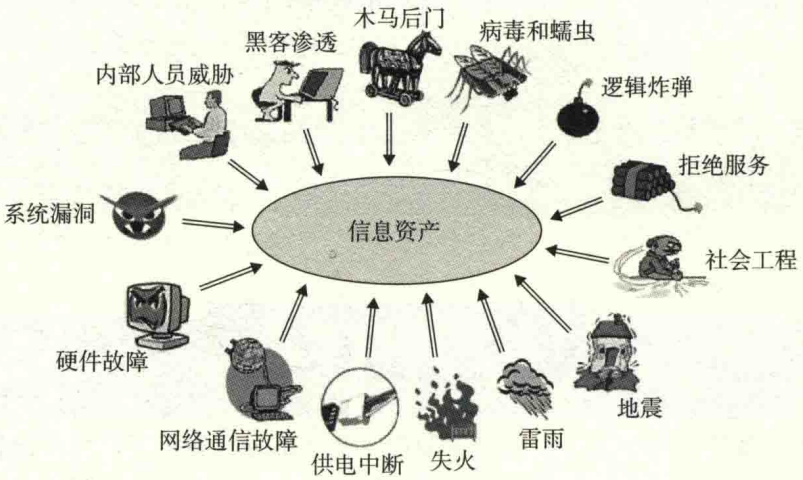

图 1－2　信息面临的安全威胁

（一）物理层安全

信息系统物理层安全风险主要包括以下方面：

（1）地震、水灾、火灾等环境事故造成设备损坏。

（2）电源故障造成设备断电以至操作系统引导失败或数据库信息丢失。

（3）设备被盗、被毁造成数据丢失或信息泄露。

（4）电磁辐射可能造成数据信息被窃取或偷阅。

（5）监控和报警系统的缺乏或者管理不善可能造成原本可以避免的事故。

（二）网络层安全

1. 数据传输风险分析

数据在传输过程中，线路搭载、链路窃听可能造成数据被截获、窃听、篡改和破坏，数据的机密性、完整性无法保证。

2. 网络边界风险分析

如果在网络边界上没有强有力的控制，则其外部黑客就可以随意出入企业总部及各个分支机构的网络系统，从而获取各种数据和信息，那么，信息泄露问题就无法避免。

3. 网络服务风险分析

一些信息平台运行 Web 服务、数据库服务等，如不加以防范，各种网络攻击可能对业务系统服务造成干扰、破坏，如最常见的拒绝服务攻击 DoS、DDoS。

（三）操作系统层安全

系统安全通常指操作系统的安全，操作系统的安装以正常工作为目标，在通常的参数、服务配置中，以及缺省地开放的端口中，存在很大的安全隐患和风险。

操作系统在设计和实现方面本身存在一定的安全隐患，无论是 Windows 还是 UNIX 操作系统，不能排除开发商留有后门（Back Door）。系统层的安全还包括数据库系统以及相关商用产品的安全漏洞。病毒也是操作系统层安全的主要威胁，病毒大多利用了操作系统本身的漏洞，通过网络迅速传播。

（四）应用层安全

（1）业务服务安全风险。
（2）数据库服务器安全风险。
（3）信息系统访问控制风险。

（五）管理层安全

管理层安全是网络中安全得到保证的重要组成部分，是防止来自内部网络入侵必需的部分。责权不明、管理混乱、安全管理制度不健全及缺乏可操作性等都可能影响管理层安全。

无论是从数据的安全性、业务服务的保障性还是从系统维护的规范性等角度，都需要对信息系统制定严格的安全管理制度，从业务服务的运营维护和更新升级等层面加强安全管理。

三、提高安全性

无论你现在使用哪种操作系统，总有一些通用的加强系统安全的建议可以参考。如果你想加固你的系统来阻止未经授权的访问和避免不幸灾难的发生，对于信息安全知识掌握较少的同学，以下预防措施肯定会对你有很大帮助。

（一）使用安全系数高的密码

提高安全性的最简单有效的方法之一就是使用一个不会轻易被暴力攻击猜到的密码。

什么是暴力攻击？攻击者使用一个自动化系统在一定范围内对所有可能的结果进行逐一排查，尽可能快地猜测密码。因此，安全系数高的密码应该包含以下两个特征：

（1）包含特殊字符和空格，同时使用大小写字母，避免使用从字典中能找到的单词，不要使用纯数字密码，这种密码破解起来比你使用母亲的名字或你的生日作为密码要困难得多。

（2）越长的密码破解越困难。你的密码长度每增加一位，就会以倍数级别增加被破解的难度。一般来说，小于 8 个字符的密码是很容易被破解的。可以用 10 个、12 个字符作为密码，16 个当然更好了。在不会因为过长而难于键入的情况下，让你的密码尽可能的长会更加安全。

密码可以设置成有规律的组合型，将英文和阿拉伯数字组合在一起，固定的部分不变，不一样的地方做出规律性的调整，这样的密码好记又安全。

（二）升级软件、打补丁

对系统进行补丁测试是至关重要的。如果很长时间没有进行安全升级，可能会导致你使用的计算机非常容易成为黑客的攻击目标。因此，不要把软件安装在长期没有进行安全补丁更新的计算机上。

同样的情况也适用于任何基于特征码的恶意软件保护工具，诸如防病毒应用程序，如果对它不进行及时更新，就不能得到当前的恶意软件特征定义，防护效果会大打折扣。

（三）关闭没有使用的服务、端口

多数情况下，很多计算机用户甚至不知道他们的系统上运行着哪些可以通过网络访问的服务，这是一个非常危险的情况。

Telnet 和 FTP 是两个常见的问题服务，如果你的计算机不需要运行它们，请立即关闭。确保了解在你的计算机上运行的每一个服务究竟是做什么的，并且知道它要运行的原因。

（四）通过备份保护数据

备份数据，这是保护自己在面临信息威胁时把损失降到最低的重要方法之一。备份数据既包括简单、基本的定期拷贝数据到 CD 上，也包括复杂的定期自动备份到一个服务器上。

（五）不要信任外部网络

在公共场合，如果是那种需要复杂密码才能连上的 Wi-Fi，可以比较放心地使用，反倒是什么都不需要，直接就可以连上的 Wi-Fi，才存在较大的安全隐患。饭馆和咖啡厅提供免费的 Wi-Fi，但这种 Wi-Fi 到底安不安全，确实很难辨别，在这种情况下上网，就需要多加注意。

因此，在公众场合使用免费 Wi-Fi 时，更多的是浏览一些信息，尽量避免一些涉及隐

私和支付的操作，如果必须进行操作，一定要确保网络环境的安全。

练一练

单项选择题

信息资产面临的主要威胁来源包括（　　）。

A. 自然灾害

B. 系统故障

C. 内部人员操作失误

D. 以上都包括

【解析】本题正确答案为 D。

经过前面的学习，如果你能够了解信息安全面临的威胁，以及自己可以对计算机进行一定的安全设置，那么恭喜你，你已经较好地掌握了本部分的内容。请记得完成在线学习活动 1。

请你做好本部分知识的梳理总结，稍做休息，我们继续进行下一个知识点的学习。

知识点 2 信息与信息安全

学前思考 2：

我们在生活中时时刻刻都要注意信息安全，信息是什么？是姓名还是身份证号码？保护信息安全到底是保护谁的信息安全？

本节知识重点

学习提示：通过知识点 1 的学习，我们知道信息面临着种种威胁。接下来，我们将继续学习信息与信息安全，之后请大家观看视频《什么是信息安全：概念与特点》，以加深对该部分内容的理解，然后完成在线学习活动 2。

信息是一种消息，通常以文字或声音、图像的形式来表现，是数据按有意义的关联排列的结果。信息安全是指信息网络的硬件、软件及系统中的数据受到保护，不受偶然的或者恶意的攻击而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，信息服务不中断。我们可以通过多方面的学习来加深对信息与信息安全的理解。

一、信息的定义

信息是事物及其属性标识的集合。信息是一种消息，通常以文字或声音、图像的形式来表现，是数据按有意义的关联排列的结果。信息由意义和符号组成，是指以声音、语言、文字、图像、动画、气味等方式所表示的实际内容。

信息是客观事物状态和运动特征的一种普遍形式，客观世界中大量地存在、产生和传递着以这些方式表示出来的各种各样的信息。在谈到信息的时候，就不可避免地涉及信息的安全问题。

二、信息的特征

信息具有很多特征，如普遍性、客观性、依附性、共享性、时效性、传递性等。下面通过对信息的一些主要特征的描述和讨论交流，来进一步认识和理解信息的概念。

（一）普遍性与客观性

在自然界和人类社会中，事物都是在不断发展和变化的，事物所表达出来的信息也是无所不在。因此，信息是普遍存在的。由于事物的发展和变化是不以人的主观意志为转移的，所以信息具有客观性。

（二）依附性

信息不是具体的事物，也不是某种物质，而是客观事物的一种属性。信息必须依附于某个客观事物（媒体）而存在。同一个信息可以借助不同的信息媒体表现出来，如文字、图形、图像、声音、影视和动画等。

（三）共享性

信息是一种资源，具有使用价值。信息传播的范围越广，使用信息的人越多，信息的价值和作用就越大。信息在复制、传递、共享的过程中，可以不断地产生副本。但是，信息本身并不会减少，也不会被消耗掉。

（四）时效性

随着事物的发展与变化，信息的可利用价值会相应地发生变化。随着时间的推移，信息可能会失去其使用价值，这时的信息就是无效的信息了。这就要求人们必须及时获取信息、利用信息，这样才能体现信息的价值。

（五）传递性

信息通过媒体的传播，可以实现空间上的传递。如我国载人航天飞船“神舟九号”与

“天宫一号”飞行器交会对接的现场直播，向全国及世界各地的人们展现了我国航天事业的发展进程，缩短了对接现场和电视观众之间的距离，实现了信息在空间上的传递。

信息通过存储媒体的保存，可以实现时间上的传递。如没能看到“神舟九号”与“天宫一号”空间交会对接现场直播的人，可以采用回放或重播的方式来收看。这就是利用了信息存储媒体的牢固性，实现了信息在时间上的传递。

三、信息安全

信息安全是指信息网络的硬件、软件及系统中的数据受到保护，不受偶然的或者恶意的攻击而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，信息服务不中断。

信息安全主要包括五方面的内容，即保证信息的保密性、真实性、完整性、未授权拷贝和所寄生系统的安全性。信息安全本身包括的范围很广，其中包括如何防范商业企业机密泄露、青少年对不良信息的浏览、个人信息的泄露等。

信息安全学科可分为狭义与广义两个层次。狭义的信息安全建立在以密码论为基础的计算机安全领域；广义的信息安全是一门综合性学科，从传统的计算机安全到信息安全，不仅是名称的变更，也是对安全发展的延伸，安全不再是单纯的技术问题，而是将管理、技术、法律等相结合的产物。

四、网络安全

从本质上讲，网络安全就是网络上的信息安全，是指网络系统的硬件、软件和系统中的数据受到保护，不受偶然的或者恶意的攻击而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。

从广义上讲，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，都是网络安全所要研究的领域。

网络安全由于不同的环境和应用而产生了不同的类型。主要类型有以下几种：

（1）系统安全。保证系统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，避免因为系统的损坏而对系统存储、处理和传输的消息造成破坏及损失；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）网络的安全。即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，计算机病毒防治，数据加密等。

（3）信息传播安全。网络上信息传播安全，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由非法、有害的信息进行传播所产生的后果，避免公用网络上的信息失控。

（4）信息内容安全。即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，其本质是保护用户的利益和隐私。

五、信息安全的目标

所有的信息安全技术都是为了达到一定的安全目标，其核心包括保密性、完整性、可用性、真实性和不可否认性五个。

（1）保密性：保证机密信息不被窃听，或窃听者不能了解信息的真实含义。

（2）完整性：保证数据的一致性，防止数据被非法用户篡改。

（3）可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝。

（4）真实性：对信息的来源进行判断，能对伪造来源的信息予以鉴别。

（5）不可否认性：建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的。

六、网络安全模型——PDRR 模型

PDRR（Protect Detect React Restore）模型中，安全的概念已经从信息安全扩展到了信息保障。信息保障的内涵已超出传统的信息安全保密，是保护（Protect）、检测（Detect）、反应（React）、恢复（Restore）的有机结合，如图 1－3 所示。

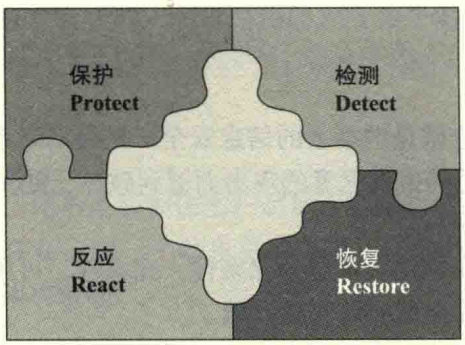

图 1－3　PDRR 模型

PDRR 模型把信息的安全保护作为基础，将保护视为活动过程，采用检测手段来发现安全漏洞，及时更正；同时采用应急响应措施对付各种入侵。在系统被入侵后，要采取相应的措施将系统恢复到正常状态，这样使信息的安全得到全方位的保障。该模型强调的是自动故障恢复能力。

现有的网络安全模型众多，不仅包括 PDRR 模型，还包括 PPDR（Policy Protection Detection Response）模型、PPDRR（Policy Protection Detection Response Restore）模型等。

练一练

单项选择题

PDRR 模型的要素不包括（　　）。

A. 保护　　B. 检测　　C. 预警　　D. 恢复

【解析】PDRR 模型是保护（Protect）、检测（Detect）、反应（React）、恢复（Restore）的结合，本题正确答案为 C。

经过前面的学习，如果你能够了解信息与信息安全的特征和定义，并了解 PDRR 模型，那么恭喜你，你已经较好地掌握了本部分的内容。请记得完成在线学习活动 2。

请你做好本部分知识的梳理总结，稍做休息，我们继续进行下一个知识点的学习。

知识点 3　信息安全的实现

学前思考 3：

即使我们在使用计算机的过程中加强防范，不随意下载内容、点击链接，但是仍然有信息安全的威胁。需要采用何种技术才能保证信息安全？请你们带着这个疑问，学习本知识点内容。

本节知识重点

学习提示：通过知识点 2 的学习，我们知道了信息与信息安全的概念和性质，也了解了存在多种信息安全模型，那么信息安全是如何实现的呢？我们需要怎样的技术？怎样进行管理？接下来，我们将学习信息安全的实现，之后请大家观看视频《什么是信息安全：实现》，加深对该部分内容的理解，然后完成在线学习活动 3。

信息安全的实现需要实施一定的信息安全策略。实现信息安全，不仅要靠信息安全技术，还要靠严格的信息安全管理、信息安全法律等来保障。

一、信息安全技术

先进的安全技术是网络安全的根本保证，常见的信息安全技术有：

（1）密码学。密码学是研究密码编制、密码破译和密钥管理的一门综合性应用学科。其中包含古典密码、对称密码、非对称密码、散列密码、数字签名等。

（2）网络安全协议。网络安全协议是营造网络安全环境的基础，是构建安全网络的关键技术。设计并保证网络安全协议的安全性和正确性能够从根本上保证网络安全，避免因网络安全等级不够而导致网络数据信息丢失或文件损坏等信息泄露问题。

（3）网络攻击技术。利用网络存在的漏洞和安全缺陷对网络系统的硬件、软件及系统中的数据进行攻击。