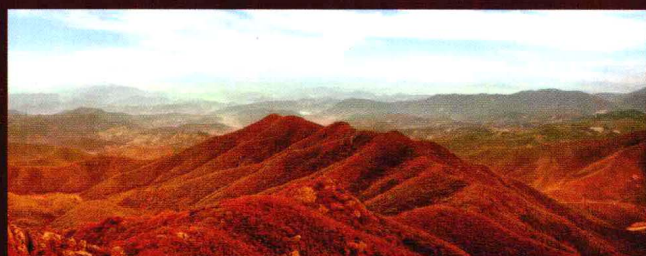


高等学校信息安全类专业系列教材

网络安全与管理



□ 陈红松 编著

清华大学出版社
北京交通大学出版社

高等学校信息安全类专业系列教材

网络安全与管理

陈红松 编著

清华大学出版社
北京交通大学出版社

·北京·

内 容 简 介

本书介绍计算机网络安全与管理技术,是面向信息安全与计算机专业的教材。本书首先从整体上介绍了网络安全与管理的基本概念、产生背景、特点及设计原则,从系统工程的角度介绍了网络安全管理的体系结构。从网络攻击技术出发,逐层次介绍了网络安全与管理的相关技术理论与标准规范。本书共分13章,内容包括网络安全与管理概述、相关规范、网络攻击与安全评估、网络安全的密码学基础、身份认证与网络安全、防火墙技术、VPN技术、入侵检测技术、面向内容的网络信息安全、电子商务安全、无线网络安全技术、网络管理原理与技术及网络信息安全的法律法规体系。

本书既可作为高等院校信息安全、计算机等相关专业的本科生和研究生相关课程的教材,也可作为网络安全管理工程技术人员的参考书。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13501256678 13801310933

图书在版编目(CIP)数据

网络安全与管理/陈红松编著. —北京:清华大学出版社;北京交通大学出版社,2010.10
(高等学校信息安全类专业系列教材)

ISBN 978-7-81123-743-6

I. ①网… II. ①陈… 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(2010)第181802号

责任编辑:谭文芳 特邀编辑:王志刚

出版发行:清华大学出版社 邮编:100084 电话:010-62776969 <http://www.tup.com.cn>
北京交通大学出版社 邮编:100044 电话:010-51686414 <http://press.bjtu.edu.cn>

印刷者:北京瑞达方舟印务有限公司

经 销:全国新华书店

开 本:185×260 印张:20.25 字数:518千字

版 次:2010年10月第1版 2010年10月第1次印刷

书 号:ISBN 978-7-81123-743-6/TP·624

印 数:1~3000册 定价:33.00元

本书如有质量问题,请向北京交通大学出版社质监局反映。对您的意见和批评,我们表示欢迎和感谢。

投诉电话:010-51686043, 51686008; 传真:010-62225406; E-mail: press@bjtu.edu.cn。

前 言

随着计算机和网络通信技术的快速发展,网络的开放性、互连性、共享程度的提高,来自外部的黑客攻击和内部的威胁使网络安全及管理问题日益突出,网络安全正面临重大挑战。本书首先介绍了网络安全与管理的基本概念、产生背景、特点及设计原则,从系统工程的角度介绍了网络安全管理的体系结构,分析了构建网络安全管理体系的必要性,注重各安全技术之间的相互作用与联系;从网络攻击技术出发,逐层次介绍了网络安全与管理的相关技术理论与标准规范。本书紧密结合当前网络信息安全领域的发展动态,体现学科前沿和研究成果,并且注重一定的实践性和创新性,每章后面都有相应习题供学生总结和复习所学知识,兼顾知识体系的完整性与系统性,本书很多内容来自编者的科研工程项目及课堂教学实践。

本书共分13章。第1章介绍网络安全与管理的基本概念、产生背景、特点及设计原则;第2章介绍网络安全与管理的体系规范与标准;第3章介绍网络攻击的概念,网络风险的识别与安全评估方法;第4章介绍网络安全的密码学基础;第5章介绍网络安全所涉及的身份认证技术与相关协议;第6章介绍防火墙的概念与原理、指标与选型、发展趋势等;第7章介绍虚拟专用网的关键技术及发展趋势,其中包括基于不同协议的VPN技术等;第8章介绍入侵检测与防护系统的关键技术以及蜜罐蜜网技术等;第9章介绍了面向内容的网络安全监控技术,并给出了论坛类网站内容安全监控模型;第10章介绍了电子商务中的安全机制以及安全电子商务协议;第11章介绍了无线网络安全技术,包括移动Ad hoc网络及无线传感器网络的安全机制;第12章介绍了网络管理原理及技术,包括SNMP/OSI网络管理框架以及新型网络管理模式;第13章介绍了网络信息安全的法律法规体系及国内外网络安全立法框架。

本书既可作为高等院校信息安全、计算机等相关专业的本科生和研究生相关课程的教材,也可作为网络安全管理工程技术人员的参考书。

本书由北京科技大学计算机系陈红松副教授主持全书内容的组织策划和统稿编写工作,黄小莉博士参与编写了其中的第4章和第10章。北京科技大学的王昭顺教授、张晓彤教授、北京邮电大学的杨义先教授、哈尔滨工业大学的傅忠传副教授等为本书的编写提供了许多宝贵建议,北京科技大学的研究生黄木、王艺璇等也参与了部分资料的收集及部分图表的制作,本书得到网络与交换技术国家重点实验室(北京邮电大学)开放课题资助(编号SKLNST-2008-1-12),中国博士后科学基金第46批资助(编号20090460245),国家自然科学基金资助(编号90818016),作者在此致以深切的感谢。

由于网络安全与管理技术发展更新较快,作者水平有限,书中的不足之处在所难免,殷切希望广大读者批评指正并提出宝贵建议和意见,以便进一步完善教材内容。编者 E-mail: architecture_ustb@yahoo.com.cn。

编 者
2010年4月

目 录

第1章 网络安全与管理概述与规划	1
1.1 网络安全与管理概述	1
1.1.1 网络安全与管理的基本概念	1
1.1.2 网络安全与管理的定义	2
1.1.3 网络安全与管理的基本属性	4
1.2 网络安全与管理问题的产生背景	6
1.2.1 网络安全问题是国际性问题	6
1.2.2 网络安全问题的根源	7
1.2.3 网络安全威胁的发展趋势	8
1.2.4 我国网络安全与管理现状	9
1.2.5 网络安全管理的必要性	11
1.3 网络安全与管理的特点及设计原则	11
1.3.1 网络安全与管理的特点	12
1.3.2 网络安全管理的设计原则	12
1.3.3 信息安全管理的原则	13
1.4 网络安全管理设计规划与实施案例	14
1.4.1 网络安全系统的设计规划步骤	14
1.4.2 银行系统网络安全设计与实施案例	15
小结	19
习题	19
第2章 网络安全与管理的体系规范	20
2.1 网络安全防范体系	20
2.2 开放系统互联安全体系结构	21
2.2.1 安全服务	22
2.2.2 特定的安全机制	23
2.2.3 普遍性安全机制	24
2.2.4 安全管理	25
2.3 Internet 网络安全体系结构	26
2.3.1 IPSec 安全协议	27
2.3.2 SSL 安全协议	30
2.4 信息保障技术框架	32
2.5 ISO/IEC 18028—2 网络安全框架	34
2.6 BS 7799 信息安全管理体系规范	35

小结	37
习题	38
第3章 网络攻击与安全评估	39
3.1 网络攻击的概念及分类	39
3.1.1 网络攻击的基本概念	39
3.1.2 网络攻击的分类	39
3.2 计算机及网络的漏洞分析	45
3.2.1 漏洞的基本概念及分类	45
3.2.2 网络漏洞	46
3.2.3 漏洞分级	46
3.2.4 漏洞的发现	47
3.3 网络脆弱性的评估技术	47
3.3.1 网络脆弱性的概念	47
3.3.2 网络脆弱性的评估	48
3.3.3 评估网络脆弱性的准则	51
3.4 信息系统安全风险的概念与评估	51
3.4.1 风险的基本概念	51
3.4.2 信息系统安全风险的概念	51
3.4.3 信息安全风险评估	52
3.4.4 风险评估指标体系的设计原则	55
3.5 网络与信息安全的风险管理	56
3.5.1 网络风险管理	56
3.5.2 信息安全风险管理	56
小结	58
习题	58
第4章 网络安全的密码学基础	59
4.1 密码学概述	59
4.1.1 密码学起源及发展阶段	59
4.1.2 密码学的基本概念	60
4.2 密码系统的设计与分析	62
4.2.1 密码系统的设计原则	62
4.2.2 密码分析的概念与方法	63
4.3 对称密码体制	65
4.3.1 对称密码体制的基本概念	65
4.3.2 对称密码体制的分类	66
4.3.3 DES 密码算法分析	69
4.4 公钥密码体制	72
4.4.1 公钥密码体制的基本概念	72
4.4.2 公钥密码体制的特点及应用	75

4.4.3	RSA 密码算法分析	75
4.5	散列函数	77
4.5.1	散列函数的基本概念	77
4.5.2	散列函数的构造方法	78
4.5.3	散列函数的密码分析	78
4.6	数字签名	79
4.6.1	数字签名的基本概念	79
4.6.2	常用的数字签名算法简介	80
4.6.3	数字签名的系统描述	80
4.6.4	数字签名及验证过程	80
4.6.5	数字签名的分类	81
4.6.6	RSA 数字签名算法	82
4.7	密钥管理	83
4.7.1	密钥管理的基本概念	83
4.7.2	密钥的使用阶段	83
4.7.3	密钥的有效期	85
4.7.4	密钥托管	85
4.8	密码学与安全协议	85
4.8.1	安全协议的基本概念	85
4.8.2	安全协议的安全性质	85
4.8.3	安全协议的缺陷分析	86
4.8.4	安全协议的分析	87
4.9	密码学在网络安全中的应用	87
4.9.1	认证的应用	88
4.9.2	电子邮件安全	88
4.9.3	IP 层安全	88
4.9.4	Web 安全	89
小结	89
习题	89
第5章	身份认证与网络安全	90
5.1	身份认证技术	90
5.1.1	身份认证技术简介	90
5.1.2	身份认证系统的特征	91
5.1.3	用户身份认证的分类	91
5.2	基于口令的身份认证	92
5.2.1	口令的存储	92
5.2.2	口令机制	92
5.2.3	对口令协议的基本攻击	93
5.2.4	口令认证的安全性	94

5.3	双因素认证技术	94
5.3.1	双因素认证原理	94
5.3.2	动态口令的产生	95
5.3.3	客户端软件代理	95
5.3.4	管理服务器	95
5.3.5	双因素身份验证系统的几个要点	95
5.4	基于 X.509 证书的身份认证	96
5.4.1	X.509 证书的格式及含义	96
5.4.2	基于 X.509 证书的双向认证过程	98
5.5	安全认证协议	98
5.5.1	NS 认证协议	98
5.5.2	Kerberos 认证协议	99
5.5.3	PAP 认证协议	101
5.5.4	CHAP 认证协议	101
5.5.5	RADIUS 认证协议	103
5.6	USB Key 身份认证	104
5.6.1	USB Key 身份认证的原理	104
5.6.2	USB Key 身份认证的特点	104
5.7	基于生物特征的身份认证	105
5.7.1	基于生物特征的认证方式	105
5.7.2	与传统身份认证技术的比较	106
5.8	零知识认证技术	107
5.8.1	零知识证明	107
5.8.2	零知识身份认证协议	108
5.9	身份认证与授权管理	108
	小结	109
	习题	109
第6章	防火墙技术	110
6.1	防火墙的概念与原理	110
6.1.1	防火墙的基本概念及工作原理	110
6.1.2	防火墙的发展历程	111
6.1.3	防火墙的主要功能	112
6.1.4	防火墙的局限性	114
6.2	防火墙的分类	114
6.2.1	按软硬件的实现形态分类	115
6.2.2	按防火墙的实现技术分类	116
6.2.3	按防火墙结构分类	122
6.2.4	按防火墙的应用部署位置分类	122
6.2.5	按防火墙性能分类	123

6.3	防火墙的体系结构	123
6.3.1	堡垒主机的基本概念	123
6.3.2	屏蔽路由器体系结构	123
6.3.3	双重宿主主机体系结构	124
6.3.4	主机屏蔽防火墙体系结构	124
6.3.5	子网屏蔽防火墙体系结构	125
6.3.6	不同结构的组合形式	125
6.4	防火墙的安全策略	125
6.4.1	防火墙安全策略的概念	125
6.4.2	防火墙安全策略的基本原则	126
6.4.3	防火墙安全策略的定制建议	126
6.5	防火墙的指标与标准	127
6.5.1	防火墙的性能指标	127
6.5.2	防火墙的功能指标	128
6.5.3	防火墙相关的国家标准	129
6.6	防火墙的配置与部署	130
6.6.1	防火墙的初始与基本配置	130
6.6.2	防火墙典型配置举例	137
6.7	防火墙的发展趋势	137
	小结	138
	习题	139
第7章	虚拟专用网技术	140
7.1	VPN 概述	140
7.1.1	VPN 的特点	140
7.1.2	VPN 的基本技术	141
7.1.3	VPN 的应用范围	142
7.1.4	企业 VPN 常见解决方案	143
7.2	VPN 的分类	144
7.2.1	按接入方式划分	144
7.2.2	按协议实现类型划分	145
7.2.3	按 VPN 的发起方式划分	145
7.2.4	按 VPN 的服务类型划分	146
7.2.5	按承载主体划分	146
7.2.6	按 VPN 业务层次模型划分	147
7.3	VPN 的设计	147
7.3.1	VPN 的安全性	147
7.3.2	VPN 的网络优化	147
7.3.3	VPN 管理	148
7.4	VPN 的安全性分析	148

7.4.1	VPN 的安全隐患	148
7.4.2	安全 VPN	149
7.5	基于 PPTP/L2TP 的 VPN 技术	151
7.5.1	PPTP 协议概述	151
7.5.2	PPTP 配置实例	152
7.5.3	L2F/L2TP 协议	158
7.6	基于 IPSec 的 VPN 技术	161
7.6.1	IPSec 协议概述	161
7.6.2	IPSec VPN 安全策略	161
7.7	基于 SSL 的 VPN 技术	162
7.7.1	SSL 协议概述	162
7.7.2	SSL VPN 的特点	162
7.7.3	SSL VPN 与 IPSec VPN 的性能比较	164
7.7.4	SSL VPN 的应用范围	165
7.8	基于 MPLS 的 VPN 技术	165
7.8.1	MPLS VPN 概述	165
7.8.2	MPLS VPN 的分类	167
7.8.3	MPLS 的工作流程	167
7.8.4	MPLS 的优点	169
7.8.5	MPLS 的标准化进展	169
	小结	170
	习题	170
第 8 章	入侵检测技术	171
8.1	入侵检测概述	171
8.1.1	入侵检测的基本概念	171
8.1.2	入侵检测的发展历史	172
8.1.3	入侵检测系统的作用及组成	173
8.1.4	入侵检测系统的优缺点分析	174
8.1.5	入侵检测系统的技术指标	175
8.2	入侵检测系统的分类	176
8.2.1	根据信息源分类	176
8.2.2	按照功能分类	178
8.2.3	根据检测方法分类	179
8.2.4	根据体系结构分类	180
8.2.5	根据检测的实时性分类	181
8.2.6	根据入侵检测响应方式	181
8.3	入侵检测系统的部署	181
8.3.1	IDS 应用部署	181
8.3.2	IDS 技术部署方式	183

8.3.3	入侵检测系统的设置步骤	183
8.4	入侵检测系统的关键技术	184
8.4.1	NIDS 的关键技术	184
8.4.2	HIDS 的关键技术	186
8.5	入侵检测系统的标准化	186
8.6	入侵防护	190
8.6.1	入侵防护系统	190
8.6.2	IDS、Firewall 和 IPS 的关系	191
8.6.3	入侵防御系统的特点	191
8.6.4	入侵防御系统的不足	193
8.7	蜜罐与蜜网技术	193
8.8	Snort 简介	193
8.8.1	概述	193
8.8.2	系统组成	194
8.8.3	工作模式	194
8.8.4	入侵检测规则及编写	196
8.8.5	部分命令	197
	小结	197
	习题	197
第9章	面向内容的网络信息安全	198
9.1	网络内容安全的概念与意义	198
9.1.1	网络信息内容安全的发展背景	198
9.1.2	网络信息内容安全监控的意义	199
9.2	网络内容安全监控的功能	199
9.3	网络信息内容安全监测的关键技术	200
9.3.1	数据获取技术	200
9.3.2	协议分析技术	202
9.3.3	应用数据还原技术	203
9.3.4	内容分析与过滤技术	204
9.4	面向内容的网络安全监控模型	206
9.4.1	系统结构模型	206
9.4.2	数据交换模型	208
9.4.3	系统管理模型	209
9.5	网络内容安全中的数据挖掘与知识发现	210
9.5.1	数据挖掘概述	210
9.5.2	网络内容安全监控中的知识发现问题	211
9.5.3	用户上网行为的关联挖掘	214
9.6	论坛类网站内容安全监控模型	216
9.6.1	BBS 问题和研究现状	216

9.6.2	BBS 内容安全监控原理	217
9.6.3	BBS 内容安全监控模型	218
小结	220
习题	220
第 10 章	电子商务安全	221
10.1	安全电子商务概述	221
10.1.1	电子商务简介	221
10.1.2	电子商务系统的结构	221
10.1.3	电子商务的安全需求	222
10.1.4	电子商务的安全体系结构	223
10.2	电子商务中的安全机制	224
10.2.1	加密技术	224
10.2.2	认证技术	224
10.2.3	网络安全技术	227
10.2.4	电子商务应用中的安全交易标准	227
10.3	电子商务的支付系统	227
10.3.1	电子支付系统简介	227
10.3.2	电子信用卡	228
10.3.3	电子现金	230
10.3.4	电子支票	231
10.4	SET 协议	232
10.4.1	SET 协议简述	232
10.4.2	SET 使用的技术	234
10.4.3	SET 证书管理	237
10.4.4	SET 流程	239
10.5	SSL 协议	241
10.5.1	SSL 协议概述	242
10.5.2	SSL 握手协议	242
10.5.3	SSL 记录协议	242
10.5.4	SSL 与 SET 的比较	243
小结	244
习题	244
第 11 章	无线网络安全技术	245
11.1	无线网络概述	245
11.2	无线网络安全概述	246
11.2.1	无线网络安全的特点	246
11.2.2	无线网络的安全隐患及配置要点	247
11.2.3	无线网络常见安全技术	248
11.3	无线局域网安全技术	249

11.4	无线移动网络安全技术	252
11.4.1	GSM 移动网络安全技术	252
11.4.2	3G 移动网络安全技术	252
11.5	无线 Ad Hoc 网络的安全技术	255
11.5.1	无线 Ad Hoc 网络简介	255
11.5.2	无线 Ad Hoc 网络的安全威胁	256
11.5.3	无线 Ad Hoc 网络的安全机制	256
11.6	传感器网络的安全技术	259
11.6.1	传感器网络简介	259
11.6.2	传感器网络的安全威胁	260
11.6.3	传感器网络的安全机制	261
	小结	263
	习题	263
第 12 章	网络管理原理与技术	264
12.1	网络管理原理及技术概论	264
12.1.1	网络管理的目标和内容	264
12.1.2	网络管理的服务层次	265
12.1.3	网络管理的功能	265
12.1.4	网络管理的组织模型	266
12.1.5	网络管理的安全问题	267
12.1.6	网络管理的标准化	267
12.2	SNMP 网络管理框架	268
12.2.1	SNMP 的由来与演变	268
12.2.2	SNMP 体系框架	269
12.2.3	管理信息结构	269
12.2.4	管理信息库	270
12.2.5	SNMP 协议的功能与发展	271
12.2.6	SNMP 的运行过程	273
12.3	OSI 网络管理框架	273
12.3.1	OSI 系统管理体系结构	273
12.3.2	公共管理信息协议	274
12.3.3	公共管理信息协议的安全性	276
12.4	电信管理网	276
12.4.1	TMN 与电信网的关系	276
12.4.2	TMN 的应用	277
12.5	新型网络管理模型	278
12.5.1	基于 CORBA 的网络管理	278
12.5.2	基于 Web 的网络管理	280
12.5.3	基于主动网的网络管理	282

12.6	CMIP、SNMP 和 CORBA 的安全性比较	283
	小结	283
	习题	283
第 13 章	网络信息安全的法律法规体系	284
13.1	网络信息安全法制建设的必要性	284
13.2	网络信息安全法律的特点	285
13.2.1	网络信息安全法应当具备的特点	285
13.2.2	我国网络信息安全法律体系存在的问题	285
13.2.3	构建完善的网络信息安全法律屏障	286
13.2.4	完善网络安全相关政策法规的对策	287
13.3	国外网络安全立法分析	288
13.3.1	各国政府网络安全立法分析举例	289
13.3.2	国外信息网络安全立法的特点	296
13.4	我国网络安全立法体系框架	297
13.4.1	我国信息网络安全法律体系	297
13.4.2	我国网络信息安全法律体系的特点	298
13.4.3	我国信息网络安全法律体系的完善	298
13.4.4	全国人大对网络安全法的修改	299
13.5	网络安全相关法律的制定与分析	300
13.5.1	《电子签名法》的制定与分析	300
13.5.2	《电子证据法》的制定与分析	302
13.5.3	《电子商务法》的制定与分析	305
	小结	308
	习题	308
	参考文献	309

第 1 章 网络安全与管理概述与规划

本章要点：

- 网络安全与管理的基本概念及意义
 - 网络安全问题的产生背景
 - 网络安全与管理的特点
 - 网络安全与管理的设计原则
 - 网络安全管理规划设计与实施案例
-

1.1 网络安全与管理概述

网络是信息社会的基础，它已经广泛深入到社会、经济、政治、文化、军事、生活等各个领域，成为人们生活中不可缺少的一部分。但由于因特网的开放性等因素，它也带来了许多安全问题，如机密信息被窃听和篡改、网络黑客攻击、计算机蠕虫病毒等，由此带来的损失和影响是巨大的。本书从网络安全与管理的角度系统阐述了相关技术及特点，并给出了一些实施案例。

1.1.1 网络安全与管理的基本概念

随着计算机和通信技术的发展，国家和社会的信息化程度逐步提高，网络已成为全球信息基础设施的主要组成部分，成为现代人工作生活中必不可少的一部分，人们对网络的依赖程度也逐步加深，一旦网络由于种种原因发生故障，陷于瘫痪，人们的生活也必然会受到极大的影响。网络技术如同一把双刃剑，在带给我们便利的同时，所引发的安全隐患问题也很值得我们关注。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所要研究的领域。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学科，它涉及安全体系结构、安全协议、密码理论、信息内容分析、安全监控、应急处理等。网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。如何更有效地保护重要的信息数据、提高网络系统的安全性已经成为所有网络应用必须考虑和解决的问题之一。

有效的网络管理不仅局限于技术上的问题，同时也是管理和法律法规的问题。网络监管系统的基础设备要采用先进的硬件设备，包括防毁、防电磁信息辐射泄露、抗电磁干扰、数据灾备及电源保护等设备。网络安全技术随着现代技术的进步不断发展，如果没有合理有效的网络管理，就难以有健康发展的网络环境。从管理上来说，目前成立专门的监管部门，分

区域分行业进行监督和管理。网络监管还必须从法律法规上进行强化,制定规范的法律法规,并达成行业和相关人员的自律。网络技术的进步给了人们以更大的信息支配能力,互联网打破了传统的区域性,使个人的网络行为对社会发生的影响空前增大,也要求人们更严格地控制自己的行为。要建立一个洁净的互联网,需要的不仅是技术、法律和管理上的不断完备,还需要网络中每个信息人的自律和自重,用个人的网络伦理道德和内在价值标准来约束自己的行为,从而自觉维护网络社会的和谐发展。

1.1.2 网络安全与管理的定义

本节给出了网络安全与管理的定义,以及网络管理的功能。

1. 网络安全的定义

国际标准化组织(International Organization for Standardization, ISO)对计算机系统安全的定义是:为数据处理系统建立和采用的技术和管理的保护,保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。由此,可以将计算机网络安全理解为:通过采用各种技术和措施,使网络系统正常运行,从而确保网络数据的可用性、完整性和保密性。所以,建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等。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,网络服务不中断。

从广义上说,网络安全包括网络硬件资源和信息资源的安全性,而硬件资源包括通信线路、通信设备(交换机、路由器等)、主机等,要实现信息快速、安全的交换,一个可靠的物理网络是必不可少的。信息资源包括维持网络服务运行的系统软件和应用软件,以及在网络中存储和传输的用户信息数据等。信息资源的保密性、完整性、可用性和真实性等是网络安全研究的重要课题。

网络安全包括一切解决或缓解计算机网络技术应用过程中存在的安全威胁的技术手段或管理手段,也包括这些安全威胁本身及相关的活动。网络安全的具体含义会随着重视“角度”的变化而变化。例如,从用户(个人、企业等)的角度来说,他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护,避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私。从网络运行和管理者的角度来说,他们希望对本地网络信息的访问、读、写等操作受到保护和控制,避免出现“陷门”、病毒、非法存取、拒绝服务以及网络资源非法占用和非法控制等威胁,制止和防御网络黑客的攻击。网络安全性就是保护网络程序、数据或者设备,使其免受非授权使用或访问,它的保护内容包括:信息和资源、客户和用户,以及私有性。

在不同的环境和应用中,网络安全的解释也不完全相同。

- ① 运行系统安全,即保证信息处理和传输系统的安全,多数是指操作系统安全。
- ② 网络上系统信息的安全,包括口令鉴别、用户存取权限控制、安全审计、计算机病毒防治和数据加密等。
- ③ 网络上信息传播的安全,即信息传播后的安全。
- ④ 网络上信息内容的安全是信息安全在法律、政治、道德层次上的要求。
- ⑤ 网络上信息本身的安全,即我们讨论的狭义的“网络安全”,其侧重于保护网络信息

的保密性、真实性和完整性。

⑥ 物理安全，即网络中各种物理设备的安全，主要是指防盗、防火、防静电、防雷击以及防电磁泄露。

从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务以及网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行有效控制。因此，网络信息安全是一个系统工程，必须综合采取各种措施才能奏效。

在网络连接能力、流通能力提高的同时，基于网络连接的安全问题也日益突出，整体的网络安全主要表现在以下几个方面：网络的物理安全、网络拓扑结构安全、网络系统安全、网络应用安全和网络管理的安全等。因此网络安全问题，应该做到防范于未然。有时不会想到自己会成为目标的时候，威胁就已经出现了，一旦发生，常常令人措手不及，造成极大的损失。

2. 网络管理的定义

网络管理就是指监督、组织和控制网络通信服务，以及信息处理所必需的各种活动的总称。其目标是确保计算机网络的持续正常运行，并在计算机网络运行出现异常时能及时响应和排除故障。一般来说，网络管理就是通过某种方式对网络进行管理，使网络能正常高效地运行。其目的很明确，就是使网络中的资源得到更加有效的利用。它应维护网络的正常运行，当网络出现故障时能及时报告和处理，并协调、保持网络系统的高效运行。

网络管理技术是伴随着计算机、网络和通信技术的发展而发展的，二者相辅相成。从网络管理范畴来分类，可分为对网“路”的管理，即针对交换机、路由器等主干网络进行管理；对接入设备的管理，即对内部计算机、服务器、交换机等进行管理；对行为的管理，即针对用户的使用进行管理；对资产的管理，即统计软硬件的信息等。

国际标准化组织在 ISO/IEC 7498—4 中定义并描述了开放系统互联（Open System Interconnection, OSI）管理的术语和概念，提出了一个 OSI 管理的结构并描述了 OSI 管理应有的行为。它认为，开放系统互联管理是指这样一些功能，它们控制、协调、监视 OSI 环境下的一些资源，这些资源保证 OSI 环境下的通信。通常对一个网络管理系统需要定义以下内容。

① 系统的功能：即一个网络管理系统应具有哪些功能。

② 网络资源的表示：网络管理很大一部分是对网络中资源的管理。网络中的资源就是指网络中的硬件、软件以及所提供的服务等，而一个网络管理系统必须在系统中将它们表示出来，才能对其进行管理。

③ 网络管理信息的表示：网络管理系统对网络的管理主要靠系统中网络管理信息的传递来实现。网络管理信息应如何表示、怎样传递、传送的协议是什么？这都是一个网络管理系统必须考虑的问题。

④ 系统的结构：即网络管理系统的结构是怎样的。

3. 网络管理的功能

国际标准化组织定义网络管理有五大功能：故障管理、配置管理、性能管理、安全管