

网络安全的特性、 机制与评价

◎ 田立勤 著

//

清华大学出版社 · 北京交通大学出版社



013038151

TP393.08
677

网络安全的特性、机制与评价

田立勤 著



清华大学出版社
北京交通大学出版社
• 北京 •

TP398.08
677



北航

C1644038

内 容 简 介

网络安全是计算机和通信领域很重要的研究方向之一,而网络安全特性及其实现机制是保障网络安全中的重要研究内容。本书分为九章,以保障计算机网络的安全特性为主线,论述实现计算机网络系统安全、计算机网络数据安全和计算机网络用户安全的三个方面的八大特性与机制,并对各个实现机制的意义、定义、导致出现安全问题的原因、评价标准、解决问题的基本思路、分类和实例等进行了详细的论述和分析。

本书全面系统地展示了网络安全特性及其实现机制的研究内容和最新成果,具有完整性、实用性和学术性。非常适合我国计算机网络和通信领域的教学、科研工作和工程应用参考。既可以供计算机、通信、电子、信息等相关专业的科研人员、研究生和大学高年级学生作为教材或教学参考书,也可以供计算机网络研究开发人员、网络运营商等网络工程技术人员参考。

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

网络安全的特性、机制与评价 / 田立勤著. —北京:清华大学出版社;北京交通大学出版社, 2013.6

ISBN 978-7-5121-1435-7

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

中国版本图书馆 CIP 数据核字(2013)第 074153 号

责任编辑:谭文芳

出版发行:清华大学出版社 邮编:100084 电话:010-62776969

北京交通大学出版社 邮编:100044 电话:010-51686414

印刷者:北京泽宇印刷有限公司

经 销:全国新华书店

开 本:175×245 印张:19.25 字数:428 千字

版 次:2013 年 6 月第 1 版 2013 年 6 月第 1 次印刷

书 号:ISBN 978-7-5121-1435-7 / TP·737

印 数:1~800 册 定价:48.00 元

本书如有质量问题,请向北京交通大学出版社质监组反映。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

背景

随着因特网、物联网的迅猛发展，信息技术在人类社会生活各方面得到广泛应用，信息网络的基础性、全局性作用日益增强。目前网络安全问题已经上升到关系国家主权和安全的高度，成为影响社会经济可持续发展的重要因素。信息通信技术的演进和发展使网络信息安全的内涵不断延伸，从最初的信息保密性发展到信息的完整性、可用性和不可否认性，进而发展到系统服务的安全性，包括网络的可靠性、可维护性、可用性、可控性及行为的可信性等，随之出现了多种不同的安全防范机制，如防火墙、入侵检测和防病毒等。虽然安全防范的技术在不断增强增多，但恶意攻击和恶意程序的破坏却并没有因此而减少或减弱。为保证信息安全，人们只好把防火墙、入侵检测、病毒防范等做得越来越复杂，但随着维护与管理复杂度的增加，整个信息系统变得更加复杂和难以维护，也使得信息系统的使用效率大大降低，因此网络正面临着严峻的安全挑战。网络的安全特性是描述和评价网络安全的重要指标，它为网络安全的定量评价与分析提供基础，其机制的实现是保障网络安全的主要途径，所以网络安全特性的准确含义、实现思路、评价标准、具体实现机制及机制的评价与改进成为提高网络安全的重要内容。

本书以保障计算机网络的安全特性为主线，论述实现计算机网络系统安全、计算机网络数据安全和计算机网络用户安全的三个方面的八大特性与机制（即，计算机网络的可靠性、计算机网络的可用性、计算机网络的可控性，用户身份可鉴别性、用户行为可信性和用户不可抵赖性，网络数据的保密性、网络数据的完整性），并对各个实现机制的意义、定义、导致出现安全问题的原因、评价标准、解决问题的基本思路、分类和实例等进行了详细的论述和分析。

本书特点与读者对象

本书具有以下鲜明特色。

（1）完整性：内容丰富全面，结构合理，体系完整，对网络安全特性与机制进行全面和系统的介绍。

（2）实用性：结合当前网络环境的特点，将网络安全特性与机制应用于云计算等新型网络应用中，给出具体的应用实例，具有很强的实用性。

（3）学术性：本书具有一定的理论高度和学术价值，书中大部分内容取材于作者近期已在国际、国内学术期刊发表的论文，全面展示了网络安全特性与机制最新的科研成果，具有很高的学术参考价值。

本书非常适合我国计算机网络和通信领域的教学、科研工作和工程应用参考。既可以供计算机、通信、电子、信息等相关专业的科研人员、研究生和大学高年级学生作为教材或教学参考书，也可以供计算机网络研究开发人员、网络运营商等网络工程技术人员参考。

致谢

作者的研究工作得到 973 计划项目(No. 2011CB311809)，国家自然科学基金(No.61163050)，新世纪优秀人才(NCET-10-0101)，中央高校基本科研项目(No. 3142013098)和青海省科技项目(No. 2012-N-525)的资助，在此表示深深的谢意！

本书的研究工作大都是在我的导师林闯教授的指导下完成的，现在所取得的成绩离不开导师对我的教诲和帮助；另外，王晓菊老师对本书进行了细致的校对，谭文芳老师在本书的写作过程中做了大量细致辛苦的工作，对此一并表示衷心的感谢！。

由于作者水平所限，加之网络安全的研究仍处于不断的发展和变化之中，书中错误和不足之处在所难免，恳请专家、读者指正。

作 者

2013 年 3 月

目 录

第 1 章 网络安全特性概述	1
1.1 网络安全与网络安全特性概述	1
1.2 网络安全含义	2
1.3 网络安全的辩证观	3
1.3.1 安全技术与安全管理在网络安全中的辩证关系	4
1.3.2 网络安全与资金投入的辩证关系	4
1.3.3 网络安全与网络性能的辩证关系	4
1.3.4 网络不安全的内因与外因及其辩证关系	5
1.3.5 加密技术在网络安全中作用的辩证关系	5
1.4 网络安全特性含义	5
1.4.1 网络的可靠性	5
1.4.2 网络的可用性	6
1.4.3 网络的可维护性	6
1.4.4 网络访问的可控性	6
1.4.5 数据的保密性	7
1.4.6 数据的完整性	7
1.4.7 用户身份的可鉴别性	7
1.4.8 用户的不可抵赖性	7
1.4.9 用户行为的可信性	7
1.5 网络不安全的根本原因	8
1.5.1 计算机系统和网络自身的脆弱性	8
1.5.2 网络和系统的开放性	8
1.5.3 威胁存在的普遍性	9
1.5.4 安全管理的困难性	10
1.6 两种网络安全基本模型与攻击方式	10
1.6.1 网络安全基本模型	10
1.6.2 P2DR 模型	11
1.6.3 网络攻击的类型	12
1.7 网络安全的服务与机制	14
1.7.1 五大网络安全服务	14

1.7.2 八大网络安全机制	15
1.7.3 安全机制与安全服务的关系对照	16
1.8 实现网络安全特性机制的评价标准	16
1.8.1 实现安全特性的机制达到安全要求的程度	16
1.8.2 实现安全特性的机制对网络性能的影响	17
1.8.3 实现安全特性的机制对信息有效率的影响	17
1.8.4 实现安全特性的机制所付出的代价	17
1.9 安全管理在保障网络安全中的重要作用	17
1.9.1 网络安全管理的具体目标	17
1.9.2 网络安全管理中的基本元素	18
1.9.3 网络安全管理原则	18
1.9.4 网络安全计划的制订有两种完全不同的策略	19

第一部分 网络系统的安全特性、机制与评价

第2章 网络可靠性实现机制与评价	21
2.1 网络可靠性概述	21
2.2 造成网络系统不可靠的原因	22
2.3 网络可靠性机制的评价标准	24
2.4 提高网络可靠性机制与评价	25
2.4.1 基于避错方法提高网络的可靠性与评价	25
2.4.2 基于容错方法提高网络的可靠性与评价	28
2.5 网络可靠性的量化评估	32
2.5.1 设备串联形成的系统可靠性评估方法	32
2.5.2 设备并联形成的系统可靠性评估方法	32
2.5.3 设备备份形成的系统可靠性评估方法	34
2.5.4 模冗余系统的可靠性评估方法	35
2.6 基于优先级的区分可靠性保障机制	35
2.6.1 区分可靠性保障的必要性	35
2.6.2 基于优先级的区分可靠性保障的基本思路	36
2.7 区分可靠性保障的关键技术——报文分类机制	37
2.7.1 区分可靠性的报文分类概述	37
2.7.2 文中用到的符号术语及报文分类定义	39
2.7.3 区分可靠性的报文分类的例子	41
2.7.4 区分可靠性的报文分类的几何解释	42
2.7.5 可用作报文分类的字段及常见的分类组合	43
2.7.6 区分可靠性的分类在网络中的位置及其模型示意图	46

2.7.7 区分可靠性的报文分类算法的衡量标准	47
2.7.8 区分可靠性的报文分类的设计原则	48
2.7.9 区分可靠性的报文分类算法的设计思路	49
2.7.10 设计高速可行的报文分类算法的思路	54
2.8 区分可靠性保障的关键技术——缓冲管理策略	56
2.8.1 缓冲管理的意义	56
2.8.2 完全划分的资源管理策略	57
2.8.3 完全共享的资源管理策略	58
2.8.4 部分共享的资源管理策略	59
2.8.5 尾部丢弃与头部丢弃策略	59
2.8.6 阈值丢弃策略	59
2.8.7 随机丢弃策略	60
2.8.8 非参数控制丢弃策略	60
2.8.9 选择性丢弃策略	60
2.8.10 缓冲管理的典型算法——RED 算法	60
2.9 区分可靠性保障的关键技术——分组调度策略	63
2.9.1 分组调度的功能	63
2.9.2 分组调度算法本质分析	64
2.9.3 分组调度算法的性能指标	65
2.9.4 静态优先级的调度策略	67
2.9.5 动态优先级的调度策略	67
2.9.6 最早截止优先的调度策略	68
2.9.7 分类分组丢失控制和实时调度的综合策略	68
第 3 章 网络可用性实现机制与评价	69
3.1 网络可用性概述	69
3.2 造成网络系统不可用的原因和评价标准	71
3.3 基于网络管理提高网络可用性	72
3.3.1 网络管理概述	72
3.3.2 网络管理的主要功能	73
3.3.3 简单网络管理协议 SNMP	76
3.3.4 对基于网络管理提高网络可用性的评价	83
3.4 基于快速检错方法提高网络可用性与评价	84
3.4.1 基于快速检错方法提高网络可用性的总结分类	85
3.4.2 措施评价	86
3.5 基于快速排错方法提高网络可用性与评价	86
3.5.1 网络系统故障的排错方法	87

3.5.2	网络故障的排错步骤	88
3.5.3	系统排错中的数据备份与恢复	88
3.5.4	基于快速排错方法提高网络可用性的总结分类	91
3.5.5	措施评价	92
3.6	常见的网络管理工具	92
3.6.1	HP OpenView	93
3.6.2	IBM NetView	94
3.6.3	SUN Net Manager	94
3.6.4	CiscoWorks	95
3.7	操作系统内置的网络故障检测的常用命令	96
3.7.1	Ping	96
3.7.2	nslookup	97
3.7.3	Tracert	98
3.7.4	Ipconfig	99
3.7.5	Winipcfg	99
3.7.6	Netstat	100
3.7.7	ARP	100
3.7.8	nbtstat	101
3.8	网络可用性的量化评估	102
3.8.1	网络可用性量化评估的基本方法	102
3.8.2	设备串联形成的系统可用性评估方法	102
3.8.3	设备并联形成的系统可用性评估方法	103
第4章	网络访问的可控性实现机制与评价	104
4.1	网络安全中网络访问的可控性概述	104
4.2	基于防火墙技术的网络访问控制机制与评价	105
4.2.1	设置防火墙的含义	105
4.2.2	防火墙分类	106
4.2.3	防火墙技术	107
4.2.4	防火墙的硬件技术架构	114
4.2.5	防火墙体系结构	114
4.2.6	对防火墙技术的评价	117
4.3	网络资源访问控制的机制与评价	119
4.3.1	用户对资源的访问控制概述	119
4.3.2	系统资源访问控制的分类	120
4.3.3	自主访问控制	121
4.3.4	强制访问控制	122

4.3.5 基于角色的访问控制	123
4.3.6 基于操作系统的访问控制	125
4.3.7 基于数据库管理系统的访问控制	128
4.3.8 用户对资源的访问控制机制的评价	129
4.4 基于入侵检测技术的网络访问控制机制与评价	130
4.4.1 入侵检测概述	130
4.4.2 入侵检测技术	131
4.4.3 入侵检测的分类	133
4.4.4 基于入侵检测技术的访问控制机制评价	134

第二部分 数据的安全特性、机制与评价

第5章 数据保密性实现机制与评价	136
5.1 网络安全中的数据保密性概述	136
5.2 数据保密性机制的评价标准	137
5.2.1 加密算法的安全（保密）强度	137
5.2.2 加密密钥的安全（保密）强度	138
5.2.3 加密算法的性能	138
5.2.4 加密的工作模式	138
5.2.5 加密算法的可扩展性	139
5.2.6 加密的信息有效率	139
5.3 基本加密技术与评价	139
5.3.1 替换加密技术与评价	139
5.3.2 置换加密技术与评价	145
5.4 加密算法的分类与评价	147
5.4.1 按密码体制分类与评价	147
5.4.2 按加密方式分类	148
5.5 数据加密标准（DES）与评价	148
5.5.1 DES 主要步骤	149
5.5.2 DES 详细步骤	150
5.5.3 数据加密标准（DES）的分析与评价	156
5.6 RSA 加密机制与评价	162
5.6.1 RSA 加解密过程	162
5.6.2 RSA 密钥的计算	163
5.6.3 RSA 的加密与解密	163
5.6.4 RSA 加密机制的分析与评价	164
5.7 RSA 与 DES 结合加密机制与评价	165

5.7.1	RSA 与 DES 结合加密机制	165
5.7.2	RSA 与 DES 相结合的加密机制的分析与评价	166
5.8	数据保密性的应用实例与作用辨析	166
5.8.1	数据保密性的应用实例	166
5.8.2	加密技术在网络安全中的作用辨析	167
第 6 章	数据完整性实现机制与评价	168
6.1	网络安全中数据完整性概述	168
6.2	数据完整性机制的评价标准	169
6.2.1	完整性验证的安全(准确)性	169
6.2.2	完整性验证中加密的安全	169
6.2.3	完整性验证算法的性能	170
6.2.4	数据完整性验证的信息有效率	170
6.3	网络安全中数据完整性验证机制与评价	170
6.3.1	基于数据校验的完整性验证机制与评价	170
6.3.2	基于消息摘要的完整性验证与评价	171
6.3.3	基于消息摘要与对称密钥加密的完整性验证机制与评价	173
6.3.4	基于非对称密钥和对称密钥结合的完整性验证机制与评价	174
6.3.5	基于对称密钥直接加密原消息的完整性验证机制与评价	174
6.3.6	基于 RSA 数字签名的完整性验证机制与评价	175
6.3.7	加密原消息作为验证码的完整性验证机制与评价	176
6.3.8	基于消息认证码(MAC)的数据完整性验证机制与评价	177
6.4	MD5 消息摘要计算算法与评价	179
6.4.1	MD5 概述	179
6.4.2	每轮的输入内容	180
6.4.3	运算前的预处理	183
6.4.4	MD5 的块处理	184
6.4.5	MD5 算法的评价	185
6.5	MD5 算法在数据安全方面的应用实例	186

第三部分 用户的安全特性、机制与评价

第 7 章	用户身份可鉴别性实现机制与评价	189
7.1	网络安全中用户身份可鉴别性概述	189
7.2	用户身份可鉴别性机制的评价标准	190
7.2.1	用户身份可鉴别机制的安全(真实)性	190
7.2.2	用户身份鉴别因素的数量和种类	190
7.2.3	口令的管理	190

7.2.4 用户身份可鉴别机制是否需要第三方参与	190
7.2.5 是否具备双向身份鉴别功能	191
7.3 用户的网络身份证——数字证书	191
7.3.1 数字证书概述	191
7.3.2 数字证书的内容	191
7.3.3 生成数字证书的参与方	193
7.3.4 证书的生成	193
7.3.5 数字证书的作用	195
7.3.6 数字证书的信任	196
7.3.7 证书吊销	197
7.4 网络安全中用户身份可鉴别性机制与评价	197
7.4.1 基于口令的用户身份鉴别机制与评价	197
7.4.2 基于口令摘要的用户身份鉴别机制与评价	199
7.4.3 基于随机挑战的用户身份鉴别机制与评价	200
7.4.4 基于口令卡的用户身份鉴别机制与评价	204
7.4.5 基于鉴别令牌的用户身份鉴别机制与评价	206
7.4.6 基于数字证书的用户身份鉴别机制与评价	208
7.4.7 基于生物特征的用户身份鉴别机制与评价	208
7.5 AAA 服务	210
7.5.1 RADIUS 协议	211
7.5.2 AAA 服务器设计	217
7.6 用户身份鉴别实例分析——U 盾	223
第 8 章 用户不可抵赖性实现机制与评价	225
8.1 网络安全中用户不可抵赖性概述	225
8.2 用户不可抵赖性机制的评价标准	226
8.2.1 不可抵赖性机制的安全性	226
8.2.2 机制是否同时具有保密性和完整性验证作用	226
8.2.3 不可抵赖性机制是否需要第三方参与	227
8.2.4 不可抵赖性机制的性能	227
8.2.5 不可抵赖性机制的信息有效率	227
8.2.6 不可抵赖性机制是否具有双向不可抵赖功能	227
8.2.7 不可抵赖性机制中的加密安全	227
8.3 用户不可抵赖性机制与评价	228
8.3.1 基于 RSA 数字签名的不可抵赖机制与评价	229
8.3.2 具有保密性的不可抵赖机制与评价	230
8.3.3 基于公钥和私钥加密体制结合的不可抵赖机制与评价	231

8.3.4 基于消息摘要的不可抵赖机制与评价	232
8.3.5 具有保密性和完整性的数字签名不可抵赖机制与评价	233
8.3.6 双方都不能抵赖的数字签名不可抵赖机制与评价	233
8.3.7 基于第三方仲裁的不可抵赖机制与评价	234
8.4 数字签名综合应用实例	236
8.4.1 Web 服务提供者安全地向用户发送信息	236
8.4.2 对等网络中两个用户的一次安全消息发送	236
8.4.3 PGP 加密技术	237
8.5 非对称密钥加密算法的中间人攻击与分析	237
8.6 几种特殊的数字签名	238
8.6.1 盲签名	238
8.6.2 不可否认签名	239
8.6.3 代理签名	240
8.6.4 群签名	240
第 9 章 用户行为可信性实现机制与评价	242
9.1 网络安全中用户行为可信性概述	242
9.2 实现用户行为可信性机制的评价标准	243
9.3 基于 AHP 的用户行为可信评估的机制与评价	244
9.3.1 用户行为可信评估的层次分解策略	244
9.3.2 用户行为可信分层量化评估的基本思路	245
9.3.3 基于 AHP 的用户行为可信评估	246
9.3.4 用户行为可信性评估的机制评价	250
9.4 基于滑动窗口的用户长期行为可信评估机制与评价	251
9.4.1 长期用户行为可信评估的原则	251
9.4.2 基于滑动窗口的用户长期行为可信评估机制	252
9.4.3 基于滑动窗口的用户长期行为可信评估机制评价	259
9.5 基于贝叶斯网络的多条件用户行为可信预测与评价	261
9.5.1 用户行为可信预测的意义	261
9.5.2 用户行为可信的贝叶斯网络模型	262
9.5.3 用户行为可信的贝叶斯网络模型	264
9.5.4 用户行为可信的等级划分和符号说明	264
9.5.5 用户行为可信的先验概率	265
9.5.6 用户行为属性的先验概率	265
9.5.7 结点的条件概率表	266
9.5.8 用户行为可信的预测	266
9.5.9 用户行为可信预测机制的评价	268

9.6 基于可信预测的用户行为博弈控制机制与评价	269
9.6.1 基于可信预测对用户行为进行博弈控制问题的提出	269
9.6.2 博弈控制的基本理论	270
9.6.3 基于用户行为可信预测的博弈控制的整体过程	272
9.6.4 文中符号说明和双方利益的得失分析	273
9.6.5 基于用户安全行为可信属性的博弈分析	274
9.6.6 基于用户行为可信预测的博弈控制策略	276
9.6.7 基于可信预测的用户行为博弈控制机制的评价	277
9.7 用户行为认证机制与评价	278
9.7.1 用户行为认证的必要性	278
9.7.2 用户行为认证概念与行为证据的获得	279
9.7.3 用户行为认证集	279
9.7.4 用户行为认证机制	284
9.7.5 用户行为认证的评价	286
9.7.6 行为认证的误报率分析	287
参考文献	288

第 1 章

网络安全特性概述

1.1 网络安全与网络安全特性概述

随着因特网、物联网的迅猛发展和信息技术在人类社会生活各方面的广泛应用，信息网络的基础性、全局性作用得到日益增强。网络已发展成为建设和谐社会的一项重要基础设施，它在通信、交通、金融、应急服务、能源调度、电力调度等方面发挥重要作用，如图 1-1 所示。

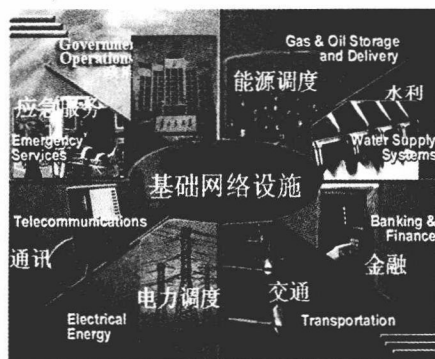


图 1-1 计算机网络的基础作用

网络安全是网络应用中重点需要解决的问题，目前网络安全已经上升到关系国家主权和安全的高度，成为影响社会经济可持续发展的重要因素。我国明确提出“加强宽带通信网、数字电视网和下一代互联网等信息基础设施建设，推进三网融合，健全信息安全保障体系”。

随着信息通信技术的演进和发展，网络信息安全的内涵不断延伸，从最初的数据保密性发展到数据的完整性、进而又发展到系统服务的安全性，包括网络的可靠性、可维护性、可用性、可控性，以及用户身份的可鉴别性、不可抵赖性和行为的可信性等，随之出现了多种不同的安全防范机制，如防火墙、入侵检测和防病毒等。虽然安

全防范的技术不断增多增强,但恶意攻击和恶意程序的破坏却并没有因此而减少或减弱。为保证信息安全,人们只好把防火墙、入侵检测、病毒防范等做得越来越复杂,但随着维护与管理复杂度的增加,整个信息系统变得更加复杂和难以维护,也使得信息系统的使用效率大大降低,因此网络正面临着严峻的安全挑战。

网络的安全特性是描述和评价网络安全的重要指标,它为网络安全的定量评价与分析提供基础,其机制的实现是保障网络安全的主要途径,所以网络安全特性的准确含义、实现思路、评价标准、具体实现机制以及机制的好坏成为提高网络安全的重要内容。

1.2 网络安全含义

定义 1.1 网络安全 网络安全泛指网络系统的硬件、软件及其系统中的数据受到保护,不因偶然的或者恶意的原因而遭到破坏、更改和泄露,系统能够连续可靠正常地运行,网络服务不被中断。

网络安全的内容包括系统安全和信息安全两部分。系统安全主要指网络设备的硬件、操作系统和应用软件的安全。信息安全主要指各种信息的存储、传输安全,具体体现在信息的保密性、完整性及不可抵赖性方面。通过采用各种技术和管理措施,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被增加、修改、丢失和泄露等。

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、数论和信息论等多种学科的综合性学科。从内容看,网络安全包括物理实体安全、软件安全、数据安全和安全管理四个方面。

1. 物理实体安全

物理实体安全主要包括以下三个方面内容。

(1) 设备安全

设备安全主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防线路截获、抗电磁干扰及电源保护等。

(2) 存储介质安全

存储介质安全的目的是保护存储在存储介质上的信息,包括存储介质数据的安全及存储介质本身的安全。

存储介质数据的安全是指对存储介质数据的保护,包括:①存储介质数据的安全删除,包括存储介质的物理销毁(如存储介质粉碎等)和存储介质数据的彻底销毁(如消磁等),防止存储介质数据删除或销毁后被他人恢复而泄露信息;②存储介质数据的防盗,是指防止存储介质数据被非法拷贝等;③存储介质数据的防毁,是指防止意外或故意的破坏使存储介质数据丢失。

(3) 环境安全

对系统所在环境的安全保护,可按照国家标准 GB 50173—2008《电子信息系统机房设计规范》和 GB/T 2887—2011《计算机场地通用规范》对网络环境进行安全设置。

2. 软件安全

软件安全又包括两个方面。

一是指软件本身是安全的,不会发生软件故障或者即使发生软件故障,该故障也不是危险的。由于软件安全漏洞带来的各种危害随着软件应用的发展日益严重,因此能有效发现并消除漏洞的软件安全漏洞发现技术也日益受到人们的重视。

二是指保护网络系统中的系统软件与应用软件不被非法复制、篡改和不受病毒的侵害等。例如,将加密技术应用于程序的运行,通过对程序的运行实行加密保护,可以防止软件被非法复制盗版以及软件安全机制被破坏。

3. 数据安全

数据安全主要指保护网络中的数据不被非法存取和破坏,确保其完整性和机密性。数据的完整性是指阻止非法实体对交换数据的修改、插入和删除;数据的保密性是指为了防止网络中各个系统之间交换的数据被截获或被非法存取而造成泄密,提供加密保护。

4. 安全管理

网络安全管理主要是以保护网络安全技术为基础,配以行政手段的管理活动。在安全问题中有相当一部分事件不是因为技术原因而是由于管理原因造成的。例如,管理规章制度的不健全、操作规程不合理和安全事件预防措施不得力等,特别是安全管理人员的误操作或恶意破坏等。只有在采取安全技术的同时,采取有力的安全管理措施才能保证网络的安全性。安全管理的对象是整个系统而不是系统中的某个或某些元素。一般来说,系统的所有构成要素都是管理的对象,从系统内部看,安全管理涉及计算机、网络、操作、人事和信息资源;从外部环境看,安全管理涉及法律、道德、文化传统和社会制度等方面的内容。确保网络安全的措施一般包括采取网络安全保障机制,建立安全管理制度,开展安全审计,进行风险分析等。

1.3 网络安全的辩证观

由于计算机网络安全不是绝对的纯技术或纯管理所能解决的问题,也不是绝对的资金投入越多越安全的问题,只有大家结合所学知识和利用辩证唯物主义理论进行思考和辨析,才能培养正确的计算机网络安全观,下面对常见的安全观点进行辩证分析。