第一图书网, tushu007.com

<<网络与通信安全技术>>

图书基本信息

书名：<<网络与通信安全技术>>

13位ISBN编号：9787115097453

10位ISBN编号：7115097453

出版时间：2002年11月1日

出版时间：人民邮电出版社

作者：刘东华

页数：394

字数：632

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

内容概要

本书在介绍网络与通信安全基本概念的基础上，重点讨论了实现网络安全的几项基本技术的原理和实现方法，并对网络和通信安全构成威胁的一些因素进行了详细地论述。
全书共分为两大部分。
第一部分为网络与通信安全技术，包括第一至第四章，主要介绍了各种密码技术、网络安全协议、防火墙技术；第二部分主要介绍对网络和通信安全构成威胁的关键因素，包括第五至第七章，主要介绍计算机病毒、特洛伊木马以及缓冲区溢出等问题。
该书不追求面面俱到，而是重点突出，主要集中在对上述几个问题的探讨，力求原理解释清楚，语言通俗易懂。

本书的主要读者对象是从事计算机网络安全和通信安全研究和开发人员，同时也可供大专院校师生学习参考，或作为相关领域的培训教材。

书籍目录

第一章　概论　1
1.1　通信安全　2
1.2　网络安全　3
1.3　安全技术　4
1.3.1　物理安全技术　4
1.3.2　信息加密技术　4
1.3.3　网络控制技术　6
1.3.4　安全协议　9
1.3.5　信息确认技术　10
1.3.6　计算机安全技术　11
1.4　法律体系的保障　13
第二章　数据加密技术　14
2.1　概述　14
2.1.1　数据加密技术及其发展　14
2.1.2　密码的抗攻击能力　16
2.2　传统密码和公钥密码研究　17
2.2.1　传统密码及一些古典密码系统　17
2.2.2　公钥密码及一些典型系统　21
2.3　DES和RSA加密算法　26
2.3.1　联邦数据加密标准(DES)算法　26
2.3.2　RSA密码体制　33
2.3.3　DES和RSA的实现　34
2.3.4　DES和RSA算法的挑战　36
2.4　刘氏高强度公开加密算法的研究　52
2.4.1　刘氏密码的设计原理　53
2.4.2　刘氏密码的算法描述　55
2.4.3　刘氏密码分析　59
2.4.4　一种基于刘氏密码的多媒体数据的加解密软件系统的设计　61
2.4.5　刘氏密码解密部分的一点探讨　63
2.5　AES密码体制　67
2.5.1　CAST-256算法　67
2.5.2　DEAL算法　70
2.5.3　CRYPTON算法　72
2.6　椭圆曲线密码算法介绍　76
2.6.1　有限域上的椭圆曲线　76
2.6.2　椭圆曲线上的密码算法　77
2.6.3　椭圆曲线密码算法的发展　78
2.7　网络加密技术方法介绍　79
2.7.1　SSL(Secure Socket Layer)　79
2.7.2　SET(Secure Electronic Transaction)　79
2.7.3　PGP(Pretty Good Privacy)　80
第三章　网络安全基础　81
3.1　TCP/IP协议　81
3.1.1　TCP/IP协议模型　81
3.1.2　TCP/IP的工作原理　82

3.1.3　网络层协议　83
3.1.4　应用层协议　87
3.1.5　传输控制协议(TCP协议)　89
3.2　接入层的安全　90
3.2.1　点到点隧道协议　92
3.2.2　二层隧道协议　94
3.3　网络层的安全　95
3.3.1　IP安全结构　95
3.3.2　IP安全协议　96
3.4　传输层的安全　101
3.4.1　安全外壳及安全套接层和传输层安全协议　102
3.4.2　SSL协议　102
3.4.3　TLS(Transport Layer Security)协议　113
3.4.4　SSL和TLS证书　117
3.5　应用层的安全　122
3.5.1　安全增强的应用协议　122
3.5.2　认证和密钥分发系统　125
第四章　防火墙技术　127
4.1　防火墙的概念和原理　128
4.1.1　防火墙的基本概念　128
4.1.2　防火墙的作用和功能　130
4.1.3　防火墙的主要技术　132
4.1.4　防火墙的组成和设置　133
4.1.5　防火墙的优缺点　136
4.1.6　防火墙的技术分类　139
4.1.7　防火墙主流产品介绍　141
4.1.8　防火墙技术的发展与展望　142
4.2　包过滤技术　149
4.2.1　屏蔽路由器　149
4.2.2　包过滤技术　150
4.2.3　包过滤型防火墙　151
4.2.4　包过滤的优点　156
4.2.5　包过滤型防火墙的缺点　156
4.3　代理技术　158
4.3.1　基本概念　158
4.3.2　代理技术　161
4.3.3　代理方式　163
4.3.4　应用网关(基于代理的)防火墙　167
4.3.5　代理防火墙的主要构件　170
4.3.6　代理防火墙的特点　173
4.4　屏蔽主机防火墙　174
4.4.1　屏蔽主机体系结构　174
4.4.2　屏蔽主机防火墙　175
4.5　屏蔽子网防火墙　176
4.5.1　屏蔽子网结构(Screened Subnet Structure)　176
4.5.2　屏蔽子网防火墙　178
4.6　双宿主机防火墙　180

4.6.1 双宿主主机结构(双宿网关)(Dual-Homed Host) 180
4.6.2 双宿网关防火墙 181
4.7 防火墙应用实例-TIS防火墙 183
4.7.1 编译运行 183
4.7.2 配置前的准备工作 184
4.7.3 配置 188
4.7.4 附加工具包 197
第五章 计算机病毒 199
5.1 计算机病毒的发展 199
5.1.1 计算机病毒的起源和发展历程 199
5.1.2 计算机病毒在中国的发展 201
5.1.3 计算机病毒产生的背景 202
5.2 计算机病毒的基本概念 203
5.2.1 计算机病毒定义 203
5.2.2 计算机病毒的分类 203
5.2.3 病毒的命名方法 208
5.2.4 计算机病毒的特点 210
5.2.5 计算机病毒产生的原因 213
5.2.6 计算机病毒的危害 214
5.2.7 计算机病毒的预防 214
5.2.8 当前计算机病毒的最新发展和特点 215
5.2.9 对计算机病毒应持有的态度 215
5.3 计算机病毒的工作机理 217
5.3.1 计算机病毒的结构 217
5.3.2 计算机病毒的传播模型 218
5.3.3 计算机病毒的运作机制 220
5.3.4 计算机病毒的触发机制 221
5.3.5 计算机病毒的传染机制 222
5.3.6 计算机病毒的引导机制 226
5.3.7 计算机病毒的破坏机制 227
5.3.8 计算机病毒的再生机制 227
5.3.9 因特网病毒 228
5.4 宏病毒 228
5.4.1 宏病毒介绍 229
5.4.2 宏病毒的生存环境 229
5.4.3 宏病毒的特点 230
5.4.4 宏病毒的危害 231
5.4.5 宏病毒的识别 232
5.4.6 宏病毒的作用机制 233
5.4.7 宏病毒传播途径 235
5.4.8 宏病毒的防治 235
5.4.9 宏病毒的清除 237
5.4.10 宏病毒举例 240
5.5 病毒的防范 244
5.5.1 计算机病毒的预防措施 244
5.5.2 病毒的防范 246
5.5.3 计算机病毒防范技术重点措施介绍 249

5.5.4　网络防病毒系统的选择　255
5.5.5　杀毒软件　257
5.6　病毒源代码示例　264
5.6.1　CIH病毒　264
5.6.2　UNIX下的计算机病毒　308
第六章　特洛伊木马　317
6.1　特洛伊木马的基本概念　317
6.1.1　特洛伊木马程序的定义　317
6.1.2　特洛伊木马程序的起源　317
6.1.3　特洛伊程序的位置　318
6.1.4　特洛伊程序的危险级别　319
6.1.5　特洛伊木马的类型　319
6.2　特洛伊程序的检测　320
6.2.1　检测的基本方法　320
6.2.2　检测工具MD5　321
6.2.3　MD5算法说明　321
6.2.4　MD5算法源代码　324
6.2.5　检测工具包　335
6.3　特洛伊木马程序的解决方法　336
6.3.1　“木马”的基本工作原理　336
6.3.2　清除“木马”的一般方法　337
6.4　特洛伊木马程序实例　338
第七章　缓冲区溢出　347
7.1　缓冲区溢出原理　348
7.2　缓冲区溢出程序的生成　350
7.2.1　在程序的地址空间里安排适当的代码的方法　351
7.2.2　控制程序转移到攻击代码的方法　351
7.2.3　代码植入和流程控制技术的综合分析　352
7.2.4　缓冲区溢出程序的生成举例　352
7.3　缓冲区溢出的保护方法　358
7.3.1　非执行的缓冲区　358
7.3.2　编写正确的代码　359
7.3.3　数组边界检查　359
7.3.4　程序指针完整性检查　360
7.3.5　程序指针完整性检查与数组边界检查的比较　362
7.3.6　防卫方法的综合分析　362
7.4　通过缓冲区溢出而获得系统特权　363
7.5　缓冲区溢出应用攻击程序及实现　371
7.5.1　Iishack.exe源代码　371
7.5.2　浏览器缓冲区溢出原理　384
7.5.3　利用此缓冲区溢出漏洞进行攻击的方法　385
7.5.4　漏洞的补救方法　386
7.5.5　dvwssr.dll远程溢出程序　386
缩略语　391
参考文献　394

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com