<<网络安全通信协议>>

图书基本信息

书名：<<网络安全通信协议>>

13位ISBN编号：9787040231229

10位ISBN编号：7040231220

出版时间：任志宇、杨艳、 陈性元 高等教育出版社 (2008-03出版)

作者：陈性元

页数：295

<<网络安全通信协议>>

内容概要

《普通高等教育"十一五"国家级规划教材·高等学校信息安全系列教材·网络安全通信协议》是普通高等教育“十一五”国家级规划教材。
《普通高等教育"十一五"国家级规划教材·高等学校信息安全系列教材·网络安全通信协议》是作者结合多年来对该课程的教学经验以及从事网络安全理论研究、产品开发及工程实践的体会编写的，从协议原理、安全性分析以及协议应用等方面，较为系统地介绍了TCP／IP协议簇各协议层的常用经典网络安全通信协议。
《普通高等教育"十一五"国家级规划教材·高等学校信息安全系列教材·网络安全通信协议》共分6大部分，共10章。
第一部分包括第一章和第二章，介绍安全通信协议的基本概念、TCP／IP协议簇的安全性问题及安全架构。
第二部分包括第三章，讨论链路层安全通信协议PPTP和L2TP。
第三部分包括第四章，讨论网络层安全通信协议IPsec协议。
第四部分包括第五章，讨论传输层安全通信协议SSL和TLS。
第五部分包括第六、七、八、九章，介绍PGP、S／MIME、SET、SNMP、S-HTTP等应用层安全协议。
第六部分包括第十章，讨论安全协议的安全性分析方法，并给出IPsec协议的分析实例。
《普通高等教育"十一五"国家级规划教材·高等学校信息安全系列教材·网络安全通信协议》不仅可作为信息安全、计算机科学与技术、密码学等专业本科高年级信息安全相关的教材，也可作为其他专业本科生和研究生的教学参考书，还可作为从事信息安全研究的工程技术人员的实用工具书。

<<网络安全通信协议>>

书籍目录

第一部分 绪论第一章 安全协议概述1.1 网络安全与安全协议1.1.1 网络安全内涵1.1.2 密码和安全协议1.2 安全协议的概念与分类1.2.1 安全协议的概念1.2.2 安全协议的分类1.3 安全协议的安全性质1.4 安全协议的设计1.4.1 安全协议的缺陷分类1.4.2 安全协议的设计原则习题一第二章 TCP／IP协议簇的安全架构2.1 TCP／IP协议簇概述2.1.1 TCP／IP协议簇协议分层2.1.2 TCP／IP协议簇基本功能保证协议2.1.3 通信协议中帧的复用和分用2.2 TCP／IP协议簇的安全性分析2.2.1 TcP／IP协议簇协议存在的安全隐患2.2.2 针对TCP／IP协议簇协议的典型攻击2.3 TCP／IP协议簇的安全架构习题二第二部分 链路层安全通信协议第三章 PPTP和L2TP协议3.1 概述3.2 PPP协议3.2.1 PPP协议基本原理3.2.2 PPP协议中的安全机制3.3 PPTP协议3.3.1 PPTP协议综述3.3.2 PPTP协议工作流程3.3.3 PPTP分组的封装3.3.4 控制消患的格式和类型3.3.5 控制连接3.3.6 呼叫3.3.7 PPTP协议中的流量控制3.4 L2TP协议3.4.1 L2TP协议综述3.4.2 12TP协议工作流程3.4.3 也TP协议消息3.4.4 控制连接3.4.5 L2TP呼叫3.4.6 L2TP的有限状态模型3.5 PPTP协议和L2TP协议分析3.5.1 PPTP协议分析3.5.2 L2TP协议分析习题三第三部分 网络层安全通信协议第四章 IPsec协议簇4.1 概述4.1.1 IPsec的产生背景4.1.2 IPsec发展概述4.1.3 IPsec的设计目标及功能4.1.4 IPsec的体系结构4.1.5 IPsec实现方式4.1.6 IPsec工作模式4.1.7 安全关联4.2 AH协议4.2.1 设计AH的目的4.2.2 AH头格式4.2.3 AH操作模式4.2.4 AH的处理过程4.3 ESP协议4.3.1 设计ESP的目的4.3.2 ESP包格式4.3.3 ESP操作模式4.3.4 ESP的处理过程4.4 IKE协议4.4.1 IKE概述4.4.2 阶段1交换4.4.3 阶段2交换4.5 IPsec若干问题4.5.1 IPsec的更小子集4.5.2 IPsec与NAT的协同4.5.3 IPsec与L2TP的结合4.5.4 IPsec在支持VPN方面的缺陷习题四第四部分 传输层安全通信协议第五章 SSL协议和TLS协议5.1 概述5.2 SSL协议规范5.2.1 协议综述5.2.2 握手协议5.2.3 更改密码规格协议5.2.4 警告协议5.2.5 SSL记录协议5.2.6 SSL协议中采用的加密和认证算法5.3 TLS协议规范5.3.1 协议综述5.3.2 TLS中的改进部分5.4 TLS／SSL的应用5.4.1 TLS／SSL与电子商务5.4.2 利用TLS／SSL保证HTTP的安全性5.5 安全性分析习题五第五部分 应用层安全通信协议第六章 电子邮件安全协议6.1 电子邮件安全概述6.1.1 电子邮件的安全需求6.1.2 安全电子邮件标准6.2 电子邮件基本原理6.2.1 电子邮件的传输机制6.2.2 电子邮件中的基本协议及标准6.2.3 MIME6.3 PGP6.3.1 PGP概述6.3.2 PGP提供的安全服务6.3.3 PGP消息格式及收发过程6.3.4 PGP的密钥管理6.3.5 PGP／MIME与OpenPGP6.4 S／MIME6.4.1 S／MIME概述6.4.2 S／MIME的安全功能6.4.3 s／MIME的消息6.4.4 S／MIME证书的处理6.4.5 增强的安全服务6.5 PGP与S／MIME的比较6.5.1 实现原理6.5.2 应用前景习题六第七章 SET协议7.1 电子商务安全概述7.1.1 电子商务概述7.1.2 电子商务的安全需求7.1.3 电子商务安全协议7.2 SET协议简介7.2.1 SET概述7.2.2 SET的安全机制7.2.3 SET的支付过程7.2.4 SET的认证7.2.5 SET的优点与存在问题7.2.6 SET的安全性分析7.3 SET与SSL的比较及SET的推广前景7.3.1 SET与SSL的比较7.3.2 SET的推广前景习题七第八章 SNMP协议8.1 SNMP概述8.1.1 SNMP产生及发展8.1.2 SNMP网络管理模型8.1.3 SNMP协议体系8.1.4 SNMP的安全问题8.2 SNMPv38.2.1 SNMPv3体系结构8.2.2 SNMPv3的消息8.2.3 SNMPv3的安全机制8.3 SNMPv3安全性分析与应用情况8.3.1 SNMPv3安全机制分析8.3.2 SNMPv3的应用情况习题八第九章 S-HTTP协议9.1 概述9.2 HTTP基本原理9.2.1 HTTP通信方式9.2.2 HTTP报文结构9.2.3 HTTP的安全机制9.3 S—HTTP9.3.1 S—HTTP概述9.3.2 S—HTTP的安全模式9.3.3 S—HTTP的消息9.3.4 其他问题9.4 S—HTTP与HTTPS的比较习题九第六部分 安全协议安全性分析第十章 安全协议安全性分析10.1 概述10.1.1 安全协议的安全性与安全性分析10.1.2 安全协议安全性分析的基本方法10.2 形式化分析10.2.1 形式化分析前提10.2.2 形式化分析基本方法10.2.3 BAN逻辑及BAN类逻辑10.2.4 SADL10.3 IPsec协议簇安全性分析实例10.3.1 IPsec协议簇安全性分析的目的与意义10.3.2 AH协议和ESP协议的安全性分析10.3.3 IKE协议安全性分析10.3.4 IPsec安全性分析小结习题十参考文献

章节摘录

插图：各字段解释如下（与以前介绍的消息相同或相近的字段不再重复介绍）：控制消息类型：取值15，表示此控制消息为SLI消息。
发送方ACCM：即远程用户发送数据时使用的ACCM。
默认为0xFFFFFFFF。
PAC将用此ACCM去掉收到的HDLC帧中的控制位。
接收方ACCM：远程用户去掉收到的HDLC帧中的控制位时使用的ACCM。
默认为0xFFFFFFFFF，在PAC物理端口上发送数据时将使用此ACCM成帧。
4．呼叫的关闭呼叫被关闭有两种原因：一是因为PAC本地的原因，此时PAC发送CDN给PNS，要求关闭会话；二是因为PNS的原因，比如远程用户通过PNS关闭会话，PNS则向PNS发送CCRQ消息，PAC在收到该消息后，回应CDN消息，确认关闭。
当远程用户请求挂断拨号访问时，应关闭相应的用户会话。
请求挂断的：PPP分组被封装后经PAC传递到PNS。
此时，PNS通过向PAC发送CCRQ消息来通知它关闭该用户的会话。
PAC收到CCRQ消息后，向PNS应答CDN消息，并关闭会话；PNS在收到CDN后，也关闭该会话。
CCRQ消息的格式如图3．29所示。

<<网络安全通信协议>>

编辑推荐

《普通高等教育"十一五"国家级规划教材·高等学校信息安全系列教材·网络安全通信协议》特色：
系统性：《普通高等教育"十一五"国家级规划教材·高等学校信息安全系列教材·网络安全通信协议》从协议产生与发展、基本原理、安全性分析、协议比较与应用等方面，较为系统地介绍了TCP／IP协议簇安全架构与各层的常用经典安全协议。
灵活性：教材体系结构相对比较灵活，不同层次的协议相对比较独立，在教学中可以根据不同专业、不同层次的教学大纲要求，选用不同章节，适当取舍后仍能形成连贯，相对完整的教材。
实用性：《普通高等教育"十一五"国家级规划教材·高等学校信息安全系列教材·网络安全通信协议》融合了作者多年来从事网络安全理论研究、产品开发及工程实践的体会。
不仅可作为信息安全、计算机，密码学等专业本科高年级学生和研究生的教材，也可作为其他专业本科生和研究生的教学参考书，还可作为从事信息安全研究的工程技术人员的实用工具书。

版权说明