<<网络安全协议>>

图书基本信息

书名：<<网络安全协议>>

13位ISBN编号：9787040253801

10位ISBN编号：7040253801

出版时间：2009-1

出版时间：高等教育出版社

作者：寇晓蕤，王清贤 编著

页数：369

前言

20世纪90年代中后期以来，信息安全一直是信息科学领域的研究热点，相关理论和技术已经逐渐成熟。
信息安全包括三个分支：存储安全、传输安全和内容安全。
本书关注传输安全，即利用网络安全协议确保信息的机密性、完整性、不可否认性，实现身份认证，并为实施访问控制提供支持。
本书定义网络安全协议为基于密码学的通信协议。
鉴于已经有很多讨论密码学的专著，本书并不关注密码学的细节，而是将安全协议作为其应用者。
此外，本书关注通信协议，这意味着每个协议都有明确的语法、语义和时序，它们体现的不仅仅是一种设计思想，而是与具体应用和特定的协议栈层次相关联。
网络安全协议已经在实际应用中发挥了重要作用。
比如，IPsec除广泛用于VPN外，已经成为IPv6使用的安全方案，在网上银行及电子商务等领域，更是能随处看到SSL（TLS）的身影。
IPsec用于IP安全，SSL（TLS）弥补了传输层协议的安全性不足。
除这两者外，TCP／IP协议族中的很多协议都有对应的安全协议标准，比如与DNS对应的DNS sec、与SNMPv1对应的SNMPv3等。
这种对应关系并不是偶然的，因为协议设计者最初关注的焦点是网络的互联互通以及直观而便捷的网络应用。
在这些问题得到很好的解决后，互联网的应用才能迅速普及。
普及的一个结果就是安全问题浮出水面，并逐渐成为下一个焦点。
在解决安全问题时，互联网的基础架构已经相当成熟并广泛部署，完全推翻这个架构并不现实。
可行的方案是针对各个协议进行安全修补，或者针对特定的需求设计新协议作为整个体系的补充。
前一种方案的结果是衍生出IPsec等与已有协议对应的安全版本；后一种方案的结果是出现了用于代理的Socks和用于认证的Kerberos等协议。
无论从体系、理论还是应用的角度看，网络安全协议的发展都已经初具规模。
虽然很多优秀的论著都涉及该方向，但国内外专门从协议的角度对其进行讨论的专著甚少。

<<网络安全协议>>

内容概要

信息安全包括三个分支：存储安全、传输安全以及内容安全。
本书关注传输安全，即利用网络安全协议保障信息安全。
本书定义网络安全协议为基于密码学的通信协议。
抛开底层密码学的细节，本书站在密码技术应用者的角度，讨论了九个TCP／IP架构下具有代表性且应用较为广泛的安全协议(或协议套件)，包括：链路层扩展L2TP、IP层安全IPsec、传输层安全SSL和TLS、会话安全SSH、代理安全Socks、网管安全SNMPv3、认证协议Kerberos以及应用安全DNSsec和SHTTP。
本书适用于计算机、通信和密码学专业的读者，既可用于教学，也可为相关工程技术人员提供参考。

<<网络安全协议>>

作者简介

寇晓蕤，博士，信息工程大学信息工程学院教师。
长期从事网络信息安全和大规模网络特性探测分析等领域的教学与研究工作。
先后主讲“网络协议分析”、“网络安全协议”等课程，获省部级科技进步一等奖1项，编写《网络协议分析》专著1本。
王清贤，信息工程大学信息工程学院网络工程系教授、博士生导师。
兼任教育部高等学校信息安全类专业教学指导委员会委员，河南省计算机学会副理事长。
长期从事网络信息安全领域的教学与研究工作。
先后主讲“网络协议分析”、“网络安全理论与技术”、“算法设计与分析”、“可计算性与计算复杂性”等十多门课程：负责国家信息安全标；隹制定工作专项中有关安全协议产品测试标准研究项目，参与负责国家863目标导向类项目“密码算法和安全协议自动化分析检测评估系统”。
获省部级优秀教学成果一等奖1项、科技进步二等奖3项以及军队院校育才奖金奖，享受军队优秀专业技术人才一类岗位津贴。

<<网络安全协议>>

书籍目录

章节摘录

插图：用于信息安全领域的散列函数应满足以下三个特性：（1）映射分布均匀性和差分分布均匀性在散列结果中，为0的比特和为1的比特，其总数应该大致相等；输入中一个比特的变化，散列结果中将有一半以上的比特改变，这又称为雪崩效应（avalanche effect）；要实现使散列结果中出现1比特的变化，则输入中至少有一半以上的比特必须发生变化。
其实质是必须使输入中每一个比特的信息，尽量均匀地反映到输出的每一个比特上去；输出中的每一个比特，都是输入中尽可能多比特的信息一起作用的结果。
（2）单向性 由数据能够简单迅速地得到其散列值，而在计算上不可能构造一段数据，使其散列结果等于某个特定的散列值，即构造相应的M=H-1（h）不可行。
这样，散列值就能在统计上唯一地表征输入值，这也是将散列值称为消息摘要（message digest）的由来，也就是要求能方便地将数据进行摘要，但在摘要中无法得到比摘要本身更多的关于消息的信息。

<<网络安全协议>>

编辑推荐

《网络安全协议:原理结构与应用》按照协议栈由底层到高层的顺序组织，将每个协议的细节，包括思想、流程及应用等内容融入整个网络安全协议的体系结构下，以便读者在通读完《网络安全协议:原理结构与应用》后，既能掌握原理，又能了解应用，既能深入细节，又能把握脉络。

<<网络安全协议>>

版权说明