<<网络安全教程>>

图书基本信息

书名：<<网络安全教程>>

13位ISBN编号：9787115204370

10位ISBN编号：7115204373

出版时间：2009-5

出版时间：人民邮电出版社

作者：田园

页数：248

<<网络安全教程>>

前言

自1976年公钥密码技术被发明以来，信息安全进入了一个思想和成果异常丰富的时代。
随着20世纪90年代网络技术全面应用，特别是因特网的普及和当前新一代无线移动网络及业务的飞速发展，网络安全开始占据信息安全领域中的核心地位，而且已成为计算机领域中发展最活跃的分支之一，创造了精彩纷呈的理论与绚丽多彩的技术成果。
也正因为如此，网络安全教学如何与时俱进，如何使初学者不仅能够较快地达到一个较高的水准，并使其知识和技能与业界当前的技术状况和未来发展趋势相一致，成为一个越来越不容易达到但又必须努力追求的目标。
本书面向初学者，但最终目标是带领读者达到一个较高的水准，即不仅掌握一定的理论知识，而且对当前网络安全领域所遇见的一些典型问题及解决这类问题的典型方法有一个较深入的理解。
为此，作者在内容的选择上不追求面面俱到：在理论基础方面，选材和阐述的原则是“够用”；在技术性内容方面，原则是“典型”和“有发展潜力”。
总的来讲本书偏重于技术和应用方面。
学习本书不需要读者具备任何安全基础知识，但考虑到网络安全是一个高度综合的领域，与计算机领域的其他分支有着丰富的联系，因此建议读者学习本书时，至少已经修完操作系统和计算机网络（包括TCP／IP及一定的网络编程知识）这些重要的专业基础课。
本书第1章汇集了关于因特网的必要的基础知识。
从第2章开始内容划分为4个部分：第1部分从入侵与反入侵的角度阐述当代网络安全领域最重要的技术之——入侵检测系统，对防火墙系统的讨论也包含在这一部分之中；第Ⅱ部分以访问控制和分布式系统中的安全策略为核心内容，并用实例具体阐述了UNIX／Linux和Java中的安全机制；第Ⅲ部分以网络安全协议为核心内容，阐述了几类当前最典型、应用最广泛的安全协议。
这部分有许多内容，特别是基于口令的密钥交换协议和组群密钥交换协议在目前尚没有其他教科书中有所讨论，但它们的重要性和应用潜力是毋庸质疑的。
这部分对密码学理论基础的阐述较为充分，而且所提供的全部材料比单纯的计算机密码学导论课程要丰富得多；第13章及最后一部分的两章内容主要适合于研究生程度或高级选修课教学，理解这些内容需要综合应用前几部分的所有知识。
把这些高级的材料组织在这里，既是出于对它们本身重要价值的考虑，也是作者想为学有余力的读者提供了解当前计算机安全理论和技术前沿的途径。
这部分内容目前尚不属于网络安全课程的“传统内容”，作者直接取自研究论文并进行了整理和加工，其中也包括作者自己的部分研究工作（13.4～13.5节中的组群密钥交换协议、15.2节中关于指数线性方程组的Q型零知识证明协议、15.3节中Boyen－Waters IBE方案的用户私钥盲生成协议和15.4节中的交集保密计算协议），建议教师不妨根据自己的兴趣和专长进行选择与补充。

<<网络安全教程>>

内容概要

本书主要介绍网络安全的理论基础和应用技术，全书内容分四个部分：第Ⅰ部分主要阐述网络入侵的典型手段及反入侵技术，包括对入侵检测和防火墙技术的深入讨论；第Ⅱ部分主要阐述分布式系统中的安全策略和访问控制技术，详细讨论了几类典型的安全策略的实现方法；第Ⅲ部分主要介绍计算机密码技术及典型的网络安全协议，详细讨论了典型的身份认证协议、基于口令的密钥交换协议、一般类型的密钥交换协议和组群密钥交换协议，还包括与此相关的应用；第Ⅳ部分介绍当代网络安全领域中的一些更高级的内容，包括安全协议的分析与验证技术、承诺协议、零知识证明协议和多方保密计算协议的典型应用。

本书内容新颖、深入浅出、实例丰富，所有的介绍都紧密联系具体的应用。

除传统内容外，本书还包括相当一部分其他教科书很少讨论的重要内容，如适合于无线传感器网络的密钥发布协议、基于口令的密钥交换协议、组群安全协议和多方保密计算协议等。

<<网络安全教程>>

书籍目录

章节摘录

插图：第1章 绪论本章首先对本书要讨论的计算机网络安全问题做一概要性的介绍，然后在第1.2节介绍因特网TcMP中最重要的技术性内容。
熟悉TCP／IP的读者可以跳过第1.2节，在需要的时候再回到这里查阅细节。
1.1 网络安全概论当前，没有人能否认计算机网络——最杰出的代表就是因特网——对人类社会带来的伟大进步，同样，也没有人敢于轻信计算机网络一因特网仍然是其最突出的例子——提供了一个值得信任的环境。
因此，计算机网络安全——当前其最主要的含义就是因特网安全——所要解决的根本问题可以表述为：如何在一个不可信任的环境下实现可信任的通信？
进而，如何在一个不可信任的环境下实现可信任的计算？
以上目标或许永远可望而不可及，实际情形更可能是在老问题不断被解决的同时，新问题和新挑战又不断出现，这或许正是科学与技术发展最引人人胜之处。
就目前而言，我们可以列举出网络环境中一些典型也是有趣的安全问题如下。
A向B声称自己是“A”，B如何验证“A”确实是A？
A、B彼此已确信对方的身份，接下来如何进行保密通信？
这里“保密”的含义是指除A、B之外的任何第三方都不能获得A、B之间传输的真正的消息。
A需要访问系统s拥有的对象o，S如何保证A的这一访问是合法的？
即使对合法访问，如何保证这一访问不会导致额外的副作用？
A拟向B购买一项B声称“只有他自己才知道答案”的秘密（信息），A如何相信B所言属实？
B又如何在不泄露这一秘密的情况下使A相信自己？
更进一步，如果B持有多条这类秘密，A却不希望B得知自己究竟对哪条秘密感兴趣，A应该如何与B完成这笔交易？
A通过网络发行其拥有产权的信息产品，A如何保证该信息仅仅被合法的用户所接收？
如果合法用户出现盗版行为（背叛），A如何毫不含糊地识别出背叛者？
更有甚者，如果多个合法用户合谋背叛，A如何能确切地识别出其中至少一个背叛者？

<<网络安全教程>>

编辑推荐

传统安全技术的透彻阐述，新一代安全技术的精辟导引，内容紧密联系实际。
《网络安全教程》阐述网络安全的基础理论和应用技术，学习《网络安全教程》只需要读者具备离散数学、计算机网络及软件技术的基础知识。
虽然《网络安全教程》面向初学者，但最终目标是带领读者达到一个较高的程度，不仅掌握一定程度的理论知识，而且对当前网络安全领域所解决的一些典型问题及解决这类问题的典型方法有一个较深入的理解。
为此，作者在内容的选择上不追求面面俱到：在理论基础方面，选材和阐述的原则是“ 够用 ”。
在技术性内容方面，原则是“ 典型 ”和“ 有发展潜力 ”。

<<网络安全教程>>

版权说明