高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

信息系统安全实验教程

刘建伟 刘培顺 赵波 陈晶 编著
陈克非 审

http://www.tup.com.cn

根据教育部高等学校信息安全类专业教学指导委员会制订的
《信息安全专业指导性专业规范》组织编写

清华大学出版社

高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥　编委会主任：肖国镇

信息系统安全实验教程

刘建伟　刘培顺　赵波　陈晶　编著

Information Security

http://www.tup.com.cn

国家重点基础研究发展计划(973计划)课题资助
(课题编号：2012CB315905)

国家自然科学基金项目资助
(课题编号：61272501)

清华大学出版社
北京

内 容 简 介

本书是国内第一本根据《信息安全专业指导性专业规范》编写的信息系统安全实验教材。本书首先设置了实验环境搭建和常用密码学算法等基础性实验，随后设置了典型操作系统安全、常用数据库安全、服务器安全、恶意代码处理和嵌入式系统安全等实验内容。

本书内容丰富，特色鲜明，实用性强，可作为信息安全、信息对抗、密码学等专业的本科生和研究生的信息系统安全实验教材，也可以作为网络安全工程师、网络管理员和计算机用户的参考书和培训教材。

图书在版编目（CIP）数据

信息系统安全实验教程 / 刘建伟等编著. —北京：清华大学出版社，2012.10
高等院校信息安全专业系列教材
ISBN 978-7-302-30054-0

Ⅰ. ①信… Ⅱ. ①刘… Ⅲ. ①信息安全—安全技术—高等学校—教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2012)第 207130 号

责任编辑：张　民　薛　阳
封面设计：常雪影
责任校对：白　蕾
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：18.75　　**字　　数**：434 千字
版　　次：2012 年 10 月第 1 版　　**印　　次**：2012 年 10 月第 1 次印刷
印　　数：1～3000
定　　价：31.00 元

产品编号：047088-01

前言

目前，国内有近百所高校都设有密码学、信息安全或信息对抗专业，许多高校已建有信息安全实验室，并系统地开设了信息安全实验课程。虽然现有的信息安全实验书籍很多，但大多数教材的内容缺乏系统性，尤其从本科教学的角度看，它们都不太适合作为信息安全实验教材。

本教材从网络安全课程教学体系出发，在实验内容编排上，力求符合教育部信息安全类专业教学指导委员会制订的《信息安全专业指导性专业规范》，满足该规范对信息安全专业本科生实践能力体系的要求。本教材将网络安全实验内容划分为“基本型实验、综合型实验、创新型实验”三个层次，由浅入深，由易到难，由简单到综合，再由综合到创新，旨在逐步培养学生的创新意识和创新能力。

本书是一本内容丰富、特色鲜明、实用性强的信息系统安全实验教材。该教材不仅包含了实验环境搭建和密码学基本算法的实验，还针对主流的操作系统如 Windows、Linux 等设置了易于理解掌握的系统安全实验；为了增强读者对整个安全系统的掌握理解，本书特别增加了常用数据库的安全实验和服务器的相关实验。此外，本教材还针对几种常见的恶意代码的处理方法设置了相关实验，力求使读者能对整个系统安全有更加系统性的了解和掌握。最后，本教材还针对嵌入式系统应用普及的现状，专门设置了嵌入式系统安全的有关实验。在每个实验的后面均附有实验报告和思考题，便于读者对实验过程和结果进行分析和总结，并对所提出的问题进行深入思考。

全书共分 3 篇 13 章。第 1 篇为计算机网络基础篇，由第 1 章和第 2 章构成，主要包括信息安全实验室网络环境建设、网络设备配置及必备基础知识等实验内容；第 2 篇为密码学篇，由第 3～7 章构成，主要包括对称密码算法、公钥密码算法、杂凑算法、数字签名算法以及常用密码软件工具使用等实验内容；第 3 篇为系统安全篇，由第 8～13 章构成。第 8 章和第 9 章为主流操作系统的系统安全实验，第 10 章和第 11 章为主流数据库及服务器安全的相关安全实验，第 12 章为常见恶意代码的处理实验，第 13 章为嵌入式系统安全实验。

本书不但可以作为密码学、信息安全、信息对抗等专业的本科生、硕士生和博士生专业课程配套实验教材，而且也可以作为信息安全工程师的培训教材。

参加本书编写的人员有刘建伟、刘培顺、赵波、陈晶等，全书由刘建伟进行了统稿和审校。本书的第 1 章和第 2 章由刘建伟编写，第 3～7 章由刘建伟、李晖和赵波编写，第 8～11 章由刘培顺编写，第 12 章由陈晶编写，第 13 章由赵波编写。

在本书的编写过程中，北京航空航天大学的张其善教授、西安电子科技大学的王育民教授、武汉大学的张焕国教授均给予作者深切的关怀与鼓励。感谢本教学团队的毛剑、尚涛、修春娣等青年教师的支持与配合。特别感谢北京航空航天大学电子信息工程学院王祖林院长、王力军老师、李昕老师，他们在北京航空航天大学信息安全实验室的建设中给予作者大力的支持和帮助。

特别感谢上海交通大学的陈克非教授。作为本书的责任编委，陈克非教授认真审阅了全书并提出了许多宝贵的意见和建议，作者在此向他表示衷心的感谢。

北京航空航天大学的陈杰、邱修峰、刘建华、刘哲、毛可飞、王朝、刘巍然等博士生和周炼赤、徐先栋、王世帅、赵朋川、张斯芸、袁延荣、樊勇、李坤、马妍、张雨霏、齐睿、张雷、童丹、张晏、冯克、苏兆安、何宇、黄福华、裴恒利、宋姗姗等硕士生，以及中国海洋大学和武汉大学的博士和硕士研究生们为提高本书的质量做了实验验证、截图升级及文字校对工作，作者在此一并向他们表示真诚的感谢。

本书得到了国家重点基础研究发展计划（973 计划）课题“可重构基础网络的安全和管控机理与结构”（2012CB315905）、军口“863 计划”项目、军口“十二五”预研项目、武器装备基金、高等学校博士学科点专项科研基金（20091102110004）以及国家自然科学基金（61272501）的支持。

尽管本实验教材积累了作者多年的实践经验和教学成果，但由于其所涉及的知识面宽广，采用的实验设备和工具种类繁多，加之时间紧、水平有限，一定存在许多不足之处，恳请广大读者批评与指正。

编　者

2012 年 8 月

目 录

第 1 篇　计算机网络基础

第 2 篇　密　码　学

第 1 篇

计算机网络基础

第1章 组网及综合布线

1.1 实验室网络环境搭建

1.1.1 实验室网络拓扑结构

信息安全实验室的硬件系统包括：

- 防火墙；
- 网络入侵检测系统（NIDS）；
- 虚拟专用网络（VPN）；
- 物理隔离网卡；
- 路由器；
- 交换机；
- 集线器。

信息安全实验室的软件系统包括：

- 脆弱性扫描系统；
- 病毒防护系统；
- 身份认证系统；
- 网络攻防软件；
- 主机入侵检测软件；
- 因特网非法外联监控软件。

信息安全实验室的网络拓扑结构如图 1-1 所示。

1.1.2 实例介绍

在实验室网络拓扑结构中，一个局域网的主机 IP 地址可按照图 1-2 设置，另外两个网络中主机的 IP 地址则按照 192.168.2.11～192.168.2.20 和 192.168.3.11～192.168.3.20 来设置。注意：一个局域网中的主机数量可以根据学生分组人数的多少来设计。在本网络安全方案设计中，假设一个班有 30 名学生，分为三组，每组 10 人。如果学生人数比较多，可以适当地增加每个局域网中主机的数目，或者增加局域网的个数。当然，这需要增加设备和投资。

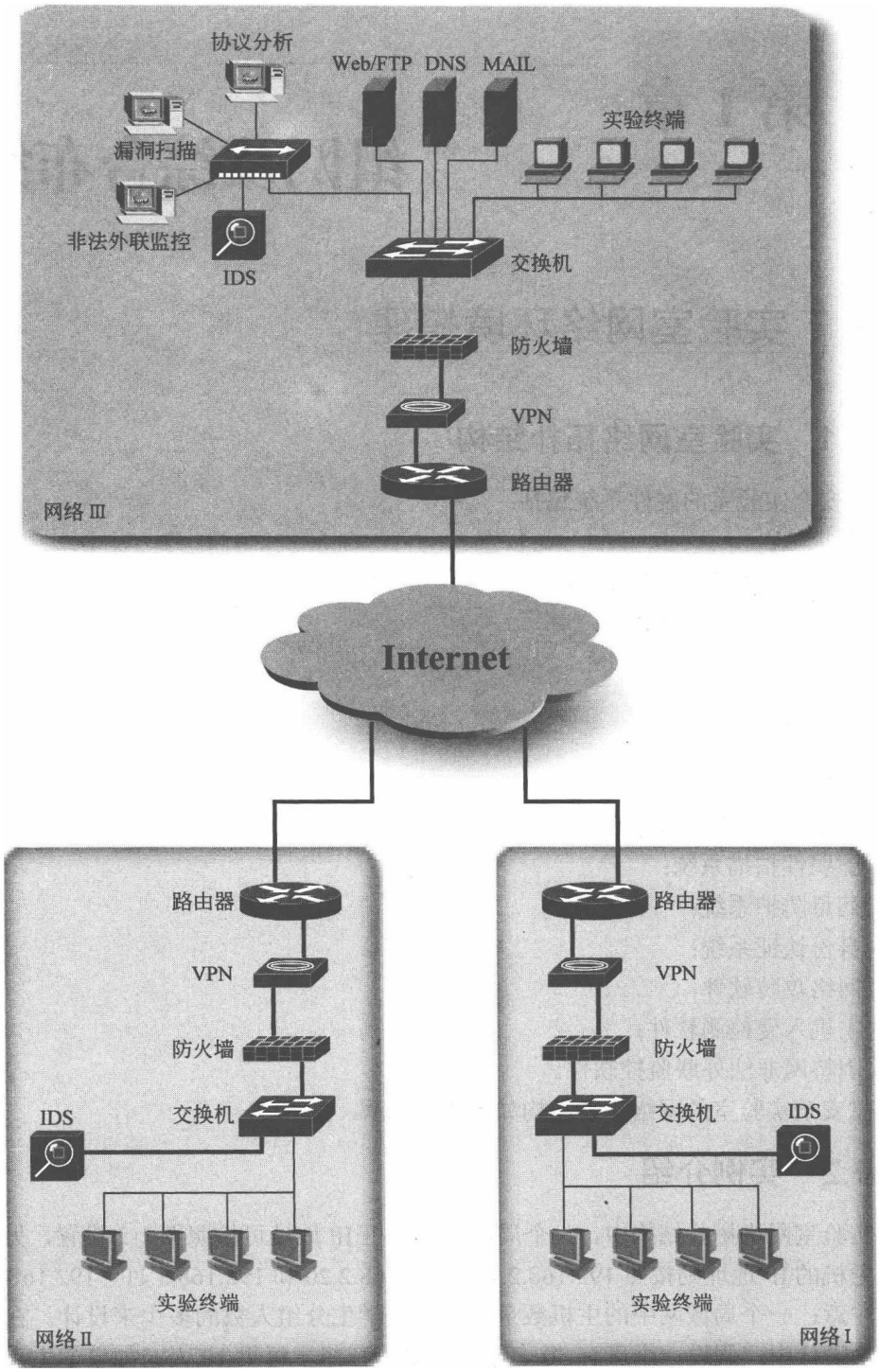

图 1-1　实验室网络拓扑结构

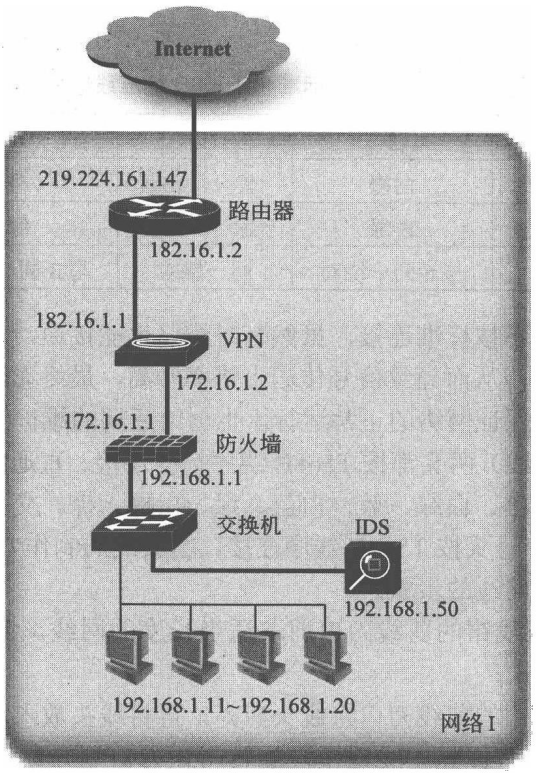

图 1-2　子网络 IP 地址设置

1.2 网络综合布线

1.2.1 网线制作

目前局域网构建已经极为普遍，小型局域网无处不在，例如家庭局域网、网吧、校园局域网和小型办公网等。在搭建网络的时候，网线的制作是需要掌握的最基本技能。网线制作的整个过程都要准确到位，排序的错误和压制的不到位都将直接影响网线的使用，导致网络不通或者网速缓慢。

超五类线是网络布线最常用的网线，分为屏蔽和非屏蔽两种。如果是室外使用，屏蔽线更合适；如果是在室内使用，一般用非屏蔽五类线就够了。由于此类线不带屏蔽层，线缆会相对柔软些，但其连接方法都是一样的。一般的超五类线里都有 4 对绞在一起的细线，并用不同的颜色标明。

双绞线一般用于星状网络的布线，每条双绞线通过两端安装的 RJ-45 连接器（俗称水晶头）将各种网络设备连接起来。双绞线的标准接法不是随便规定的，目的是保证线缆接头布局的对称性，这样就可以使接头内线缆之间的干扰相互抵消。双绞线有两种接法：EIA/TIA 568B（T568B）标准和 EIA/TIA 568A（T568A）标准。两种标准的线序如

表 1-1 所示。

表 1-1 T568A 标准和 T568B 标准线序表

标准	1	2	3	4	5	6	7	8
T568A	白绿	绿	白橙	蓝	白蓝	橙	白棕	棕
T568B	白橙	橙	白绿	蓝	白蓝	绿	白棕	棕
绕对	同一绕对		与 6 同一绕对	同一绕对		与 3 同一绕对	同一绕对	

制作网线时，如果不按标准连接，虽然有时线路也能接通，但是线路内部各线对之间的干扰不能有效消除，从而导致信号传送出错率升高，最终影响网络整体性能。只有按规范标准建设，才能保证网络的正常运行，也会给后期的维护工作带来便利。

直通线（也叫作正线）两头都按 T568B 线序标准连接。直通线的两端线序一样，即从左至右线序是白橙、橙、白绿、蓝、白蓝、绿、白棕、棕。交叉线（也叫作反线）一头按 T568A 线序连接，一头按 T568B 线序连接。交叉线的制作方法与直通线相同。

下面介绍制作直通网线的步骤。

（1）剪断：利用压线钳的剪线刀口剪取适当长度的网线。截取双绞线长度至少为 0.6m，最多不超过 100m。

（2）剥皮：用压线钳的剪线刀口将线头剪齐，再将线头放入剥线刀口，让线头触及挡板，调整好长度，稍微握紧压线钳慢慢旋转，让刀口划开双绞线的保护胶皮，拔下胶皮。

（3）排序：剥除外包皮后即可见到双绞线网线的 4 对 8 条芯线，按照规定的线序排列整齐。

（4）剪齐：把线尽量抻直（不要缠绕）、压平（不要重叠）、挤紧理顺（朝一个方向紧靠），然后用压线钳把线头剪平齐。外层去掉外层绝缘皮的部分约为 14mm，这个长度正好能将各细导线插入到各自的线槽。如果该段留得过长，一来会由于线对不再互绞而增加串扰，二来会由于水晶头不能压住护套而可能导致电缆从水晶头中脱出，造成线路的接触不良甚至中断。

（5）插入：一只手以拇指和中指捏住水晶头，使有塑料弹片的一侧向下，针脚一方朝向远离自己的方向，并用食指抵住；另一只手捏住双绞线外面的胶皮，缓缓用力将 8 条导线同时沿 RJ-45 头内的 8 个线槽插入，一直插到线槽的顶端。

（6）压制：确认所有导线都到位，并透视水晶头检查一遍线序无误后，就可以用压线钳压制 RJ-45 头了。将 RJ-45 头从无牙的一侧推入压线钳夹槽后，用力握紧线钳（如果力气不够大可以使用双手一起压），将突出在外面的针脚全部压入水晶头内。

（7）测试：把水晶头的两端都做好后即可用网线测试仪进行测试，如果测试仪上 8 个指示灯都依次为绿色闪过，证明网线制作成功。如果是直通线，测试仪上的灯应该是依次顺序闪亮；如果做的是交叉线，那么测试仪的闪亮顺序应该是 3、6、1、4、5、2、7、8。

另外，在购买双绞线时请注意：应该选用的是五类双绞线。三类线的传输距离只能达到 16m，四类线只能达到 20m，只有五类线以及超五类线等才能到达 100m。

在布线时，要注意：对每条网线要采用号卡子（一种塑料卡子）在网线的两头做适当标识。可以按照局域网和分组进行编号。例如，若网线连接的是第一个局域网的第 5 台主机，那么可以在网线两头的线卡子上编号为 A5。这样，可以保证网线不会出现混乱，且便于查找故障。

在机柜中，各设备之间的连线也要采用恰当的标识加以区分。实验室工作人员可以根据具体情况自行设计编号。

1.2.2　设备连接

1. 网卡与网卡

网卡之间直接连接，可以不用集线器（Hub），应采用交叉线连接。

2. 网卡与光收发模块

将网卡装在计算机上，做好设置；给收发器接上电源，严格按照说明书的要求操作；用双绞线把计算机和收发器连接起来，双绞线应为交叉线接法；用光跳线把两个收发器连接起来，如收发器为单模，跳线也应用单模的。光跳线连接时，一端接 RX，另一端接 TX，如此交叉连接。不过现在很多光模块都有调控功能，交叉线和直通线都可以用。光纤收发器基本网络连接如图 1-3 所示。

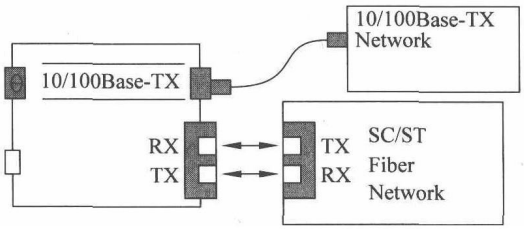

图 1-3　光纤收发器基本网络连接图

3. 光收发模块与交换机

当用双绞线把计算机和收发器连接起来时，采用直通线连接。

4. 网卡与交换机

当网卡与交换机相连时，采用直通线连接。含有网卡的设备包括 PC、VPN、防火墙，入侵检测系统、路由器等设备。

5. 集线器与集线器（交换机与交换机）

当两台集线器（或交换机）通过双绞线级联时，必须要用交叉线。这种情况适用于那些没有标明专用级联端口的集线器之间的连接。但是，有许多集线器为了方便用户，提供了一个专门用来串接到另一台集线器的端口。在对此类集线器进行级联时，应采用直通线连接。

6. 交换机与集线器

交换机与集线器之间也可通过级联的方式进行连接。级联通常是解决不同品牌的交换机之间以及交换机与集线器之间连接的有效手段。

7. VPN 和防火墙，VPN 和路由器，防火墙与路由器

它们之间的连接与 PC 之间连接类似，使用交叉线。

8. 计算机串口与路由器/交换机/防火墙/VPN 等设备的 RJ-45 控制口连接

当采用计算机的串口对以上网络设备进行管理时，需要在 PC 的串口上安装一个串口/RJ-45 转换器。这样，就可以采用一条直通线连接 PC 和网络设备的 RJ-45 控制口。注意：串口/RJ-45 转换器的引脚线序排列有可能不同。各设备随机附件中提供的串口/RJ-45 转换器可能不同。因此，在设备安装时，切记不要把这些串口/RJ-45 转换器张冠李戴。