普通高等教育“十一五”国家级规划教材　计算机系列教材

教育部信息安全特色专业建设项目

网络安全协议

赖英旭　杨震　刘静　编著
李健　审

清华大学出版社

普通高等教育“十一五”国家级规划教材　计算机系列教材

教育部信息安全特色专业建设项目

赖英旭　杨震　刘静　编著

网络安全协议

清华大学出版社

北京

内 容 简 介

本书比较全面地介绍了网络安全协议的关键技术和主要应用模式。特别对 VPN 网络的特点、分类及应用模式等方面进行了比较深入的分析和探讨。

本书对数据链路层安全协议、网络层安全协议、传输层安全协议、会话层安全协议和应用层安全协议等方面进行了比较深入的分析，并介绍了各层协议的安全缺陷、易受到的攻击以及在相应层协议中所增强的安全机制。在网络安全协议应用方面，本书重点阐述了 3 种常见的 VPN 网络应用模式，并比较详细地介绍了 VPN 网络的工作原理和配置。

本书通俗易懂，注重可操作性和实用性。通过对典型 VPN 网络应用模式案例的讲解，使读者能够举一反三。本书可作为广大计算机用户、计算机安全技术人员的技术参考书，特别是可用做信息安全、计算机与其他信息学科本科生的教材，也可用做计算机信息安全职业培训的教材。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目（CIP）数据

网络安全协议/赖英旭，杨震，刘静编著. —北京：清华大学出版社，2012.10
（计算机系列教材）
ISBN 978-7-302-27903-7

Ⅰ. ①网… Ⅱ. ①赖… ②杨… ③刘… Ⅲ. ①计算机网络－安全技术－通信协议－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2012)第 008916 号

责任编辑：汪汉友
封面设计：常雪影
责任校对：梁　毅
责任印制：李红英

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：北京密云胶印厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：15.5　　**字　　数**：370 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：26.00 元

产品编号：035509-01

网络安全一直是一个倍受关注的领域。如果缺乏一定的安全保障，无论是公共网络还是企业专用网络，都难以抵挡网络攻击和非法入侵。如果没有适当的安全措施和访问控制方法，在网络上传输的数据很容易受到各式各样的攻击。本书主要介绍从数据链路层到应用层，安全协议在保证数据传输安全性方面所采取的关键技术。

本书由北京工业大学从事教育部“信息安全”特色专业建设的教师编写（从事大学本科网络安全协议教学 6 年、研发工作 6 年）。书中重点分析了网络安全协议的运行机制，并采用大量案例讲解安全协议的应用。

本书分为 9 章，具体内容如下。

第 1 章　安全标准。介绍国内外主要的安全评价标准，重点介绍国际上通用的信息技术安全性评价通用准则（CC），并通过介绍流行操作系统的等级，使读者更加清晰地了解信息技术安全性评价通用准则的使用。

第 2 章　数据链路层安全协议。本章首先介绍了原有数据链路层协议的安全问题，为了增强数据链路层协议的安全性，着重介绍了局域网数据链路层安全协议 IEEE 802.10 和 IEEE 802.1q、广域网数据链路层安全协议 L2TF 和 PPTP 以及无线网数据链路层安全协议 IEEE 802.11 和 IEEE 802.1x。

第 3 章　网络层安全协议。本章介绍网络攻击的特点及危害和工作原理等。为了让读者更充分了解网络层安全协议的技术特征，又详细地介绍网络安全协议 IPSec 的体系结构，IPSec 所包含的安全协议、安全联盟和密钥交换等关键技术。

第 4 章　传输层安全协议。本章详细分析传输层安全协议 SSL 的握手协议和记录协议。此外，还对 SSL 的安全性进行了分析。

第 5 章　会话层安全协议。本章介绍会话层安全协议 SSH 的主要安全机制、SSH 身份认证协议和 SSH 连接协议。为了使读者对 SSH 协议的应用理解得更加深入，还对 SSH 的典型应用案例进行了介绍。

第 6 章　应用层安全协议。本章介绍安全电子邮件协议和 S-HTTP 协议，使读者了解为了降低应用层协议受到的攻击，在应用层安全协议中所采用的安全机制。

第 7 章　VPN 基础。本章介绍安全协议最重要的应用——构建 VPN 网络，内容包括 VPN 的工作原理、特点和分类。重点讲述了 VPN 的 3 种应用模式：构建企业内部虚拟网络、构建企业外部虚拟网络和远程接入虚拟网络。

第 8 章　VPN 应用案例。本章通过 A 公司和某高校网络两个案例，介绍 3 种 VPN

应用模式的配置要点，为构建安全网络体系提供解决方案。

第9章　VPN产品介绍和选购标准。本章对国内外流行的VPN产品进行了介绍，给出各产品的技术特点，并在最后给出了公司构建虚拟专用网络(VPN)时的选购标准。

本书由北京工业大学赖英旭、杨震、刘静和杨胜志共同编写，其中第1章～第3章由赖英旭编写，第4章～第6章由杨震编写，第7章和第9章由刘静编写，第8章由杨胜志编写。全书最后由赖英旭和杨震统稿，李健审定。

本书的研究和编写工作受到教育部和北京市“信息安全特色专业建设项目”资助。本书从各种论文、图书、期刊以及互联网中引用了大量的文献资料，在文字的录入和整理中得到了李健老师的帮助，在此谨表示衷心感谢。

由于时间和水平有限，书中难免有误，恳请读者批评指正，使本书得以改进和完善。

作　者

2012年6月

FOREWORD

此为试读，需要完整PDF请访问：www.ertongbook.com

《网络安全协议》目录

此为试读,需要完整PDF请访问: www.ertongbook.com

第1章 安全标准

为了对现有计算机系统的安全性进行统一评价，为计算机系统制造商提供一个权威的系统安全性标准，需要有一个计算机系统安全测评标准。美国国防部于1983年推出了历史上第一个计算机评价准则——《可信计算机系统评价准则》(TCSEC)，带动了国际上计算机安全测评的研究。随后，各国也相继发布了自己的信息安全技术标准：欧盟发布了信息技术安全评价标准(ITSEC)、加拿大发布了加拿大可信计算机产品评价标准(CTCPEC)、美国发布了信息技术安全联邦标准(FC)等。这些标准基本上都采用了TCSEC的安全框架和模式，将信息系统的安全性分成不同等级，并规定了不同等级应实现的安全功能或安全措施，它们之间的关系可用图1-1来表示。近年来，我国也制定了相应的强制性国家标准和推荐标准。

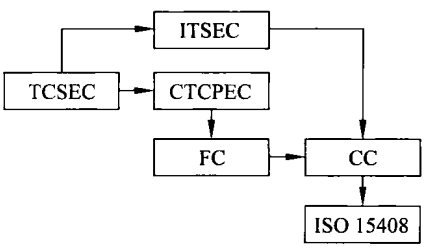

图1-1 评测标准关系图

下面列出了几个常用的安全标准。

(1) 美国TCSEC。美国国防部于1983年制定，提供D、C1、C2、B1、B2、B3、A1这7个等级的可信系统评价标准，每个等级对应有确定的安全特性需求和保障需求，高等级需求建立在低等级需求的基础之上。

(2) 欧洲ITSEC。1991年，西欧四国制定了信息技术安全评价规则(ITSEC)，ITSEC首次提出了信息安全的保密性、完整性和可用性概念，把可信计算基的概念提高到可信信息技术的高度上来认识。它定义了从E0～E6这7个安全等级和10种安全功能。

(3) 联邦标准FC。由美国国家标准与技术协会和国家安全局联合开发的拟用于取代TCSEC标准的计算机安全评价标准。该标准把安全功能和安全保证分离成两个独立的部分，并提出了保护轮廓定义书和安全目标定义书的概念。该标准只有草案，没有正式版本。

(4) 通用准则CC。1993年6月，美国、加拿大及欧洲4国经协商同意，起草单一的通用准则(CC)，并将其推进到国际标准。CC结合了FC及ITSEC的主要特征，它强调将安全的功能与保障分离，并将功能需求分为9类63族，将保障分为7类29族。

(5) GB 17859—1999。中国国家技术监督局参考TCSEC和可信计算机网络系统说明(NCCS)而制定的国家强制标准，共分5个安全等级。

(6) GB/T 18336—2001：中国国家技术监督局参考CC标准而制定的国家推荐标准，共分为3个部分：简介和一般模型、安全功能要求和安全保证要求。

1.1 国内外发展现状

1.1.1 TCSEC

1983年，美国国防部颁布了历史上第一个计算机安全评价标准，这就是著名的可信计算机系统评价标准，简称TCSEC，又称橙皮书。1985年，美国国防部对TCSEC进行了修订。

如图1-2所示，TCSEC定义了7个等级(D，C1，C2，B1，B2，B3，A1)组成的4个类别，类A中的级别A1是最高安全级别，类D中的级别D是最低安全级别。类别用来度量提供安全保护的程度，每一个级别和类别都是在前一个基础上增加条款形成的。TCSEC还给出了与安全政策、责任、保障和文档相关的两条明确可操作的评估准则，并给出了TCSEC的测试需求。TCSEC准则的原理是在C1级别设立基本安全要求，然后在高安全级别的每一层都加入新的需求。TCSEC引入了“可信计算机基(TCB)”和“安全内核(或引用监视器)”两个重要概念，TCB是硬件、固件和实施某项安全政策的软件的组合表示，是安全机制的抽象。“安全内核(或引用监视器)”是硬件、固件和软件的组合，该软件不仅实现访问控制功能，而且保护自己免受篡改。“安全内核”实现了系统安全政策的强制访问控制功能，是安全机制的具体实现。TCSEC要求安全模型A1级别的设计必须通过形式化的数学证明，形式化的安全模型在今天仍然具有重要性，形式化可用于安全系统的需求说明和设计验证。

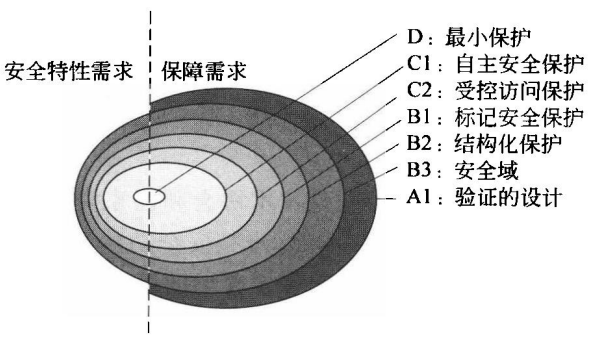

图1-2 TCSEC的构成与等级结构

7个等级的安全特性需求分别如下。

D ：最小保护

C1：自主安全保护

C2：受控访问保护

B1：标记安全保护

B2：结构化保护

B3：安全域

A1：验证的设计

TCSEC的初衷是主要针对集中式计算的分时多用户操作系统。这套计算机安全的规范与测试评估标准发布之后不久，人们就发现很难将橙皮书应用于网络(分布式)或数据库管理系统(客户服务器结构)。当分布式处理形成规范时，美国国防部又颁布了对橙皮书的附加说明和解释，提高了TCSEC标准的实用范围。

1.1.2 ITSEC、CTCPEC及FC

1. ITSEC

TCSEC测评标准应用于非操作系统类比较困难，要求安全产品为了达到某个评估级别，底层操作系统必须完全满足相应的功能要求。新范式的思想就是将通信保密和计算机安全合为一体，通称为信息安全，用于保护信息免受偶然或恶意的非法泄密、转移或破坏，这就是20世纪80年代末出现的ITSEC。ITSEC将安全性要求分为“功能”和“保证”两部分。其中，“功能”指为满足安全需求而采取的一系列技术安全措施，如访问控制、审计、鉴别、数字签名等；“保证”指确保“功能”正确实现及其有效性的安全措施。

ITSEC根据保证要求定义了7个评估级别：E0～E6。

E0：无要求。

E1：有安全目标和TOE的描述，满足安全目标的测试。

E2：要求具体设计的描述，测试证据需要加以评估、配置管理、分发控制。

E3：需要进行源代码和结构评估，安全机制的测试证据需要加以评估。

E4：安全策略模型，需要有安全增强功能、架构设计和详细设计。

E5：具体设计和源代码必须相符，并需要使用源代码进行漏洞分析。

E6：TOE的强制标准、安全策略模型的实施。

功能要求在测定上分F1～F10共10级。1～5级对应于TCSEC的D到A，6～10级加上了以下概念。

F6：数据和程序的完整性。

F7：系统可用性。

F8：数据通信完整性。

F9：数据通信保密性。

F10：包括机密性和完整性的网络安全。

表1-1所示为ITSEC和TCSEC的简单对比。

表1-1 ITSEC和TCSEC的简单对比

级别	ITSEC	TCSEC	级别	ITSEC	TCSEC
1	E0	D	5	F4＋E4	B2
2	F1＋E1	C1	6	F5＋E5	B3
3	F2＋E2	C2	7	F5＋E6	A1
4	F3＋E3	B1			

2. CTCPEC

加拿大可信计算机产品评估准则 CTCPEC vol 1.0 于 1989 年公布，专为政府要求而设计。CTCPEC 将安全分为功能性要求和保证性要求两部分。功能性要求为机密性、完整性、可用性和可控性 4 个大类。每种安全要求又分成多级，用于表示安全性上的差别，并按程度不同分为 0～5 级。

3. FC

FC 基于 MSFR 和加拿大的 CTCPEC，其中 MSFR 是 FC 针对 TCSEC 的 C2 级要求提出了适用于商业组织和政府部门的最小安全功能要求。在此标准中首先引入了“保护轮廓(PP)”这一重要概念，每个保护轮廓都包括功能部分、开发保证部分和评测部分，规定了信息产品或系统的技术要求，主要供美国政府使用、民用和商用。

1.1.3 GB 17859—1999

GB 17859—1999 是我国在参考 TCSEC 的基础上制定的国家强制标准，1999 年由国家质量技术监督局发布。GB 17859—1999 规定的计算机系统安全保护能力的 5 个等级分别对应于 TCSEC 中的 C1 级至 B3 级。它在用户自主保护级，即最低级别设立基本安全要求，然后在每一个高安全级别都加入新的需求。

该标准从自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、数据完整性、隐蔽信道分析、可信路径和可信恢复 10 个方面将计算机信息系统安全保护等级划分为 5 个安全等级。

第 1 级：用户自主保护级，用户自主保护级的计算机信息系统。可信计算基通过隔离用户与数据，使用户具备自主安全保护的能力。安全机制包括自主访问控制、身份鉴别、数据完整性。

第 2 级：系统审计保护级。与用户自主保护级相比，系统审计保护级的计算机信息系统中，可信计算基实施了粒度更细的自主访问控制。它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。安全机制包括自主访问控制、身份鉴别、客体重用、审计、自主数据完整性策略。

第 3 级：安全标记保护级，安全标记保护级的计算机信息系统。可信计算基具有系统审计保护级的所有功能。此外，还需要提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述。具有准确地标记输出信息的能力，消除通过测试发现的任何错误。安全机制包括自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、自主和强制数据完整性策略。

第 4 级：结构化保护级，结构化保护级的计算机信息系统。可信计算基建立于一个明确定义的形式化安全策略模型之上，它要求将第 3 级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的计算机信息系统可信计算基必须结构化为关键保护元素和非关键保护元素；计算机信息系统可信计算基的接口也必须

明确定义，使其设计与实现能经受更充分的测试和更完整的复审；加强了鉴别机制，支持系统管理员和操作员的职能，提供可信设施管理，增强了配置管理控制。系统具有相当的抗渗透能力。安全机制包括自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、自主和强制数据完整性策略、隐蔽通道分析、可信路径。

第5级：访问验证保护级，访问验证保护级的计算机信息系统。可信计算基满足访问监控器需求，访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的，必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算基在构造时，排除那些对实施安全策略来说并非必要的代码，在设计和实现时，从系统工程角度将复杂性降低到最小程度；支持安全管理员职能，扩充审计机制，当发生与安全相关的事件时，发出信号；提供系统恢复机制；系统具有很高的抗渗透能力。安全机制包括自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、自主和强制数据完整性策略、隐蔽通道分析、可信路径、可信恢复。

1.1.4 GB/T 18336—2001

《GB/T 18336—2001 信息技术　安全技术　信息技术安全性评估准则》是中国国家质量技术监督局于2001年发布的推荐标准，该标准的安全功能要求以类、族、组件来表达。类用于对安全要求进行最一般的分组，类中成员覆盖不同的安全目标，但都有一个共同的安全焦点；族包括一套安全要求，满足一个安全目标，但在侧重点和严格性上有差别；组件是族的成员，它描述一个明确的安全要求，是标准定义结构中最小的可选安全要求。标准提供了11个功能类，包括安全审计类、通信类、密码支持类、用户数据保护类、标识与鉴别类、安全管理类、隐秘类、TFS保护类、资源利用类、访问类和可信路径/通道类。以安全审计类为例，它共包括以下6族。

(1) 安全审计自动响应：在检测到可能有安全侵害一类事件时发生的响应。

(2) 安全审计数据产生：对于在TFS控制下发生的安全相关事件，记录其出现的要求。

(3) 安全审计分析：为寻找可能的或真正的安全侵害，用来分析系统活动和审计数据的自动化措施的要求。

(4) 安全审计查阅：可供授权用户查阅审计数据的审计工具的要求。

(5) 安全审计事件选择：在TOE运行期间选择事件来审计的要求。

(6) 安全审计事件存储：TFS能够创建并维护安全的审计踪迹的要求。

1.2 信息技术安全评估通用标准

进入20世纪90年代中期，信息技术安全评估通用标准CC产生，它是加拿大、法国、德国、荷兰、英国和美国6个国家共同努力的成果。CC标准是现阶段最完整的信息技术安全性评估准则。

CC标准将信息技术安全要求分为“功能”和“保证”两大部分。“功能要求”是对产品提供的安全功能或特征的描述，“保证要求”能够让用户相信功能要求能够得到满足，这与

许多国际标准中的区分相类似。CC 定义了安全功能要求的类、族和组件结构划分，提出了常见安全功能要求的 11 个功能类的 135 个功能组件，给 CC 标准的使用者提供直接的参考。用户可以从该结构中选择合适的组件，来定义他们对产品的安全功能要求，编制保护轮廓 PP；开发人员可以选择适当组件定义产品的安全功能，编制安全规范 ST；测评人员同样可以选择适当的组件定义测评内容、编制包。CC 的这种结构形式使得制定标准具有很好的结构性和可操作性。标准起草人仅对部分组件提出了详细具体的规范，对不能详尽规范的组件，只提出了初步的规定，将组件的具体规范留给了标准使用者。CC 也定义了安全保证要求的类、族和部件的结构划分，用于保障 IT 产品或系统满足它的安全目标，安全保证需求使用评估保证级别(EAL)进行区别。

与早期的评估准则相比，CC 的特点体现在其结构的开放性、表达方式的通用性以及结构、表达方式的内在完备性和实用性 4 个方面。

CC 的最基本思想是基于可信的 IT 产品或系统评估，为用户使用产品或系统提供信心保证。

1.2.1 CC 安全测评体系分析

CC 是一个庞大的体系，仅文档就有 1111 页。国内的很多操作系统测评是建立在 CC 标准上的，所以非常有必要对 CC 标准的使用方法以及用 CC 标准进行安全测评的方法、流程和步骤进行分析和总结。

CC 标准的全称是 Common Criteria for Information Technology Security Evaluation，即信息技术安全性评价通用准则。CC 体系一共包括 3 大部分，分别是 Common Criteria for Information Technology Security Evaluation(CC)信息技术安全性评价通用准则、Common Methodology for Information Technology Security Evaluation(CEM)信息技术安全评价通用方法和 Common Criteria Recognition Agreement(CCRA)通用准则识别协议。整个 CC 体系可以通过其官方网站 http://www.commoncriteriaPortal.org 获取。

1. CC 概要

CC 为 IT 产品提供了一系列通用的安全功能需求和安全保证需求，它可以用做安全功能的 IT 产品开发、评价和采购的指导。CC 的体系结构如图 1-3 所示。

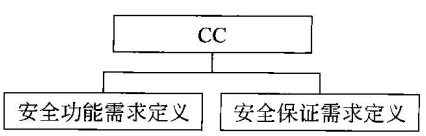

图 1-3 CC 体系结构图

CC 分为 3 个部分，每个部分的内容如下。

第 1 部分：简介和一般模型。该部分是 CC 的总体结构简介，定义了信息技术安全性评估的一般概念和原理，并提出了评估的一般模型。整个评估的过程都要遵循这个一般模型。

第 2 部分：安全功能组件。该部分建立了一系列功能组件，作为 TOE 基本功能需求的标准模板。

第 3 部分：安全保证组件。该部分建立了一系列保证组件，作为 TOE 基本保证需求的标准模板。该部分包括 PP 和 ST 的评价准则等安全保证需求，而且介绍 7 个被称为评

此为试读，需要完整PDF请访问：www.ertongbook.com