电子科技大学规划教材
电子科技大学高水平教材
电子科技大学创新创业学院选定教材

网络安全协议

NETWORK SECURITY PROTOCOLS

主　编　秦　科
副主编　娄春伟　张　力　曹明生

电子科技大学出版社
University of Electronic Science and Technology of China Press

电子科技大学规划教材
电子科技大学高水平教材
电子科技大学创新创业学院选定教材

网络安全协议

NETWORK SECURITY PROTOCOLS

主　编　秦　科
副主编　娄春伟　张　力　曹明生

电子科技大学出版社
University of Electronic Science and Technology of China Press
·成都·

图书在版编目(CIP)数据

网络安全协议 / 秦科主编. -- 成都：电子科技大学出版社，2019.3
ISBN 978-7-5647-6721-1

Ⅰ. ①网… Ⅱ. ①秦… Ⅲ. ①计算机网络－安全技术－通信协议 Ⅳ. ①TP393.08
中国版本图书馆CIP数据核字（2019）第009329号

网络安全协议
WANGLUO ANQUAN XIEYI

主　编　秦　科
副主编　娄春伟　张　力　曹明生

策划编辑　周清芳
责任编辑　周清芳
出版发行　电子科技大学出版社
　　成都市一环路东一段159号电子信息产业大厦　邮编 610051
主　　页　www.uestcp.com.cn
服务电话　028-83203399
邮购电话　028-83201495

印　　刷　四川永先数码印刷有限公司
成品尺寸　170mm×240mm
印　　张　13.5
字　　数　300千字
版　　次　2019年3月第一版
印　　次　2019年3月第一次印刷
书　　号　ISBN 978-7-5647-6721-1
定　　价　38.00元

作者简介

秦科，博士，副教授，博士生导师，爱好中国古典文学的纯正理工男。长期从事神经网络与机器学习、大数据、信息安全等领域的研究。主持完成了国家自然科学基金、四川省科技厅国际合作交流、科技支撑、应用基础重点等多项纵向项目和横向行业应用项目。担任多个SCI期刊审稿人；发表高水平论文30余篇。主讲本科专业课程《计算机操作系统》和核心通识课程《人类文明经典赏析——从红楼梦探究国学》；面向留学生主讲《Security Protocols》。曾获得电子科技大学第七届“本科教学优秀奖”，电子科技大学第七届教学成果奖二等奖，连续四次获得“来华留学研究生培养优秀任课教师”等奖项。编写教材2本：《信息安全概论》、《网络安全协议》，建设国家级精品课程《计算机操作系统》一门。

本书编委会

主　　编： 秦　科

副 主 编： 娄春伟　　张　力　　曹明生

编 委 会： 洪　磊　　陈大江　　陈　伟

黄　丹　　李贞昊　　刘　伟

陈　亚

前言

PREFACE

通信协议的安全已经成为当前互联网应用中的一个核心问题，也是信息安全领域一直高度关注并大力研究的一个热点课题。网络安全协议的目的就是通过正确地使用加密技术来解决网络通信的安全问题。目前，该领域的研究热点在于如何构建高可信网络体系。本书为入门知识教材，通过对网络安全协议中的基本理论、概念、类型和研究方法的分析介绍，试图为读者建立起网络安全协议的全面轮廓和初步概念，为进一步深入研究协议的安全性打下良好的基础。

全书共分10章，按照从理论到应用的思想，将全书分为三个部分：

第一部分是网络安全协议基本理论，包括第1章绪论；第2章密码学基础，主要讨论密码编码的基本算法；第3章认证协议和密钥建立协议，从原理角度讨论身份认证的各种方法以及多种密钥建立协议的步骤；第4章特殊数字签名与阈下信道，主要讨论特殊数字签名的基本原理；第5章其他安全协议，介绍了安全协议中的零知识协议、智力扑克协议、公平投币协议、不经意传输协议、非否认协议等。

第二部分对当前已经被广泛应用的网络安全协议进行了介绍，包括第6章IPsec协议，讨论了IPsec的体系结构、基本要素和工作原理及模式；第7章Kerberos协议与X.509证书，介绍当前网络通信中最有名的两种安全认证协议：即Kerberos协议与X.509证书的原理和实现；第8章SSL协议，主要讨论SSL协议的细节。

第三部分是网络安全协议的基本分析研究方法，包括第9章安全协议分析与设计，主要讨论了安全协议的形式化分析技术以及安全协议的设计技术；第10章介绍了当前国内外主要的安全规范与标准。

本书的部分章节内容涉及数论的基本知识原理，但都不复杂，作者在撰写过程中力求以通俗易懂的语言将安全协议的基本原理展示给读者。

本书根据秦科的讲稿凝练修改而成，凝结了作者多年的教学经验，但由于水平有限，书中难免有疏漏之处，恳请读者斧正。

编　者

2019年2月

目录

CONTENTS

第一章 绪 论

CHAPTER ONE
INTRODUCTION

1.1 基本概念

协议（Protocol）泛指国家、政府、政党、团体间关于某一问题经谈判、协商后取得的一致意见，例如国家间的关税贸易协议、个人与开发商之间的房屋买卖协议等。以现实生活中简化的房屋买卖协议为例，我们来考察协议一般要涉及的内容，如图1-1所示。

房屋买卖协议书

甲方（卖方）：

乙方（买方）：

丙方（中介方）：房地产置业服务处

一、甲方自愿将坐落在_____号的房屋，建筑面积_____平方米，出售给乙方。

二、甲、乙双方议定的上述房屋成交价格为人民币（大写）_____（元），乙方由_____年____月____日前，一次付给甲方。

三、双方同意于_____年____月____日由甲方将上述房屋交付给乙方所有。

四、甲方保证上述房屋产权清楚，若发生与甲方有关的产权纠纷，由甲方承担责任。

五、办理房屋过户手续所缴纳的税费，由甲、乙双方负担。

六、本协议经双方签字盖章后，经房地产交易主管机关审核，该房屋产权归乙方所有。

七、甲、乙双方同意委托丙方承办此件代理服务。

八、本协议一式三份，甲、乙、丙各执一份。

甲方（签字）：章

乙方（签字）：章

年　月　日

图1-1　房屋买卖协议书

图1-1中内容是经三方面对面谈判、协商，并取得一致意见后，形成的书面文本，经多方签字盖章后生效。

随着计算机网络技术的应用与发展，电子商务、电子政务已深入我们的生活。可以说每个人都已经或多或少地参与到利用互联网来实现信息交换和网络资源共享。而实现信息交换和资源共享需要一系列的协议，比如通信协议、安全协议等。这些协议同现实生活中的协议有很多相同之处，当然也有较大的区别。

在计算机网络中，为了使计算机或终端之间能够正确地传递信息，必须有一整套关于信息传输顺序、信息格式和信息内容等的约定，这一整套约定称为通信协议。网络通信协议主要由以下三要素组成：

语法（Syntax）：数据与控制信息的结构与格式。

语义（Semantics）：需要发出何种控制信息，以及要完成的动作与作出的响应。

时序（Timing）：对事件实现顺序的详细说明。

例如，我们熟悉的TCP协议，就详细规定了语法（报文格式）、语义（例如拥塞控制）、时序（例如三次握手报文序列）。

协议，就是两个或多个参与者为了完成某一项任务而采取的一系列步骤。以图1-1的房屋买卖为例，我们来分析这个定义包含的三层意思。

首先，两个或多个参与者意味着协议的完成至少需要两人的参与。单独一个人不能完成协议，一个人不能实现房屋的买卖。或者说，由一个人就可以完成的动作约定，不能称为协议。

其次，一系列步骤意味着在参与者之间表现为消息处理、消息交换交替进行的有序操作。每一步都必须依次完成。例如，买卖双方必须按照法律规定的手续一步步办理房屋过户。

最后，参与者之间合作执行协议是为了完成某一项任务或者达成某一种共识。例如，上面的房屋买卖协议就是为了完成一次交易。

除此之外，协议还具有以下一些特点。

➢协议中的每一方都必须了解协议，并且预先知道要完成的所有步骤和要达到的目的。例如，房屋买卖的双方都清楚知道他们买卖的目的，卖方是为了赚钱，买方是为了居住，并且买卖双方都知道应该办理什么手续。

➢协议签订后，每一方都必须遵循协议规定，如果一方不遵循，协议就会中断，另一方就可能会提起法律诉讼以维护自己的利益。

➢协议必须清晰没有歧义。在协议的编写必须咬文嚼字，必须明确协议中每一个字、每一个词的确切所指。

➢协议必须是完整的，对每种可能的情况必须规定具体的应对措施。

类似的，在计算机和通信世界里，协议也必须同样满足以上特点。表1-1对房屋买卖协议和TCP协议做了一个比较。

表1-1　协议比较

	房屋买卖协议	TCP协议
参与者	买方、卖方、中介	连接的发起者、响应者
步骤	按照法定程序依次完成	按照三次握手依次完成
目的	完成房屋所有权转换	建立一个连接

计算机网络中如果只有通信协议是远远不够的。为了保证信息交换的安全，现代电子商务、电子政务、网上银行都必须要有安全协议的参与。什么是安全协议呢？安全协议也被称为密码协议，它建立在密码体制之上，运行于计算机网络或分布式系统中。安全协议借助于密码算法，为安全需求的各方提供一系列规范化的步骤来达到密钥分配、身份认证、确认消息接收/发送或安全完成电子商务交易等目的。

按照安全协议所要达到的目的不同，可以将安全协议分为以下几类：

➢密钥交换协议（Key Exchange Protocol）

这类协议用于完成会话密钥（Session Key）的建立。一般情况下是在参与协议的双方或多方之间建立共享密钥，如用于一次通信中的会话密钥。协议的密码算法可以采用对称密码算法，也可以采用非对称密码算法。这类协议往往不单独使用，而是与认证协议相结合。

➢认证协议（Authentication Protocol）

认证协议包括身份认证协议、消息认证协议、数据源认证协议和数据接收认证协议等，主要用于防止假冒、篡改、抵赖等攻击。

➢认证和密钥交换协议（Authentication and Key Exchange Protocol）

这类协议将认证协议和密钥交换协议相结合，先对通信实体的身份进行认证，在成功认证的基础上，再为下一步安全通信分配将要使用的会话密钥。它是网络安全应用中最普遍的一种安全协议。常见的认证和密钥交换协议有：因特网密钥交换协议（Internet Key Exchange Protocol，IKE）、分布式认证安全服务（Distributed Authentication Security Service，DASS）协议、Kerberos协议等。

➢电子商务协议（Electronic Commerce Protocol）

与上述协议最为不同的是，电子商务协议中，其交易双方的利益目标不一致或根本就是矛盾的。电子商务协议最关注的是公平性，即协议应保证交易双方都不能通过损害对方的利益而使自己获益。常见的电子商务协议有SET（Secure Electronic Transfer）协议等。

1.2 信息安全的目标

信息安全的基本目标是保障信息处理、传输和存储的安全。不同的应用场合，信息安全技术提供的安全服务是不同的。通常来说，信息安全应提供以下四种安全服务：机密性（Confidentiality）、完整性（Integrity）、认证性（Authority）和不可抵赖（Non-repudiation）。

机密性：指保护消息内容不被泄漏给非授权拥有此消息的人，即使是攻击者观测到了消息的格式，他也无法从中提取消息的内容或得到任何有用的信息。实现机密性的最重要手段就是采用加密算法对消息进行加密。

完整性：指防止消息的内容受到任何非法修改、删除或替代。最常用的方法完整性保护是采用封装和签名，即用加密的方法或Hash函数产生一个明文的摘要附在传送消息上，作为验证消息完整性的依据，也称为完整性校验值。

认证性：是最基础的安全性质之一，所有其他安全性质都依赖于此认证的实现，认证包含两方面含义：对消息本身的认证和对实体的认证。

不可抵赖（Non-repudiation）：也称不可否认，即用户不可否认敏感的消息或文件。当由于某个实体否认它曾经执行过某项操作的时候，就需要启动不可否认服务。不可否认性包含接收方不可否认、发送方不可否认等。

除以上四个服务外，信息安全技术还应提供诸如匿名性（Anonymity）、可用性（Usability）、可审查性（Auditability）和可控制性（Controllability）等安全服务。密码学为这些服务提供了基础支撑作用，如加解密算法、Hash函数、数字签名，以及基于这些基础算法的安全套件。

1.3 Dolev-Yao攻击模型

可以毫不夸张地说：在网络中，攻击无处不在！我们经常都听到这样一些名词：拒绝服务攻击、重放攻击、ARP攻击……我们把网络攻击从广义上划分成两类：被动攻击和主动攻击。

被动攻击：攻击者只能窃听网络上的数据，对数据不做任何修改。被动攻击者只能对数据的机密性构成威胁。

主动攻击：攻击者不仅能窃听网络上的数据，而且试图修改这些数据，如删除、篡改、增加、重放等。主动攻击者能对数据的机密性、完整性、认证性等构成威胁。这是一类强大的敌人。

我们所使用的操作系统（Windows、Linux、MacOS等）、计算机网络都是一些开放系统。既然是开放系统，任何人都可以调用系统提供的接口，利用计算机网络发送和接收消息。我们必须认识到，使用计算机以及网络的人可以分为两

类：一类是诚实的人，他们具有良好的素质，遵循法律、道德和标准，只利用相应的工具和资源做合理合法的事。在本书中，我们将这类人命名为Alice、Bob、Carlos等。而另一类，我们将之称为恶意者，他们可能具备高超的能力，精通操作系统、密码学、通信等各种技术，能窃听网络上的数据，能对这些数据进行删除、修改、复制、重放等，从而达到自己期望的结果。在本书中，我们将这类人命名为Eve。

Dolev和Yao做出了一个假定：Eve可能是一个人，也可能是一个团伙。他们相当聪明，并且精通网络通信的各种技术细节。他们的行为不一定遵循法律、道德和标准，他们可以作出任何我们意料不到的事。这样一个强大的对手可以视作恶意网络的化身。这就是被广泛采纳的Dolev-Yao攻击模型。在该模型中，如图1-2所示，发送到网络中的任何消息都可以看作是发给Eve的；任何接收方收到的消息都可以看作是经过Eve处理的；Eve可以随心所欲地进行主动或者被动攻击。

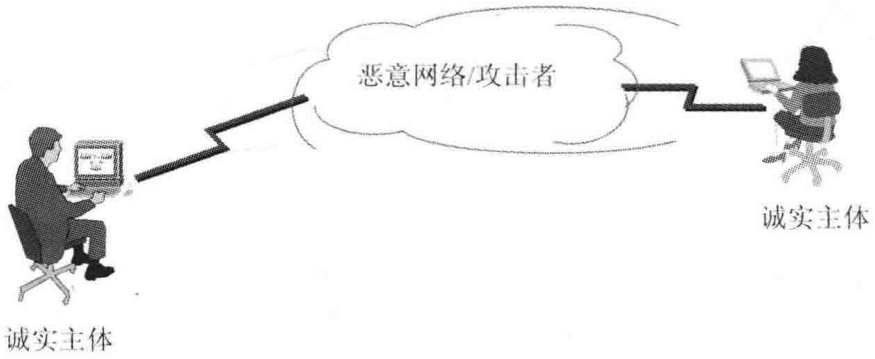

图1-2　Dolev-Yao攻击模型

尽管Eve如此强大，但他也不是万能的。比如，以下一些事情就是Eve所不能做的。

- Eve不能够在不知道密钥的情况下恢复明文的内容；同样，Eve也不能在不知道密钥的情况下，构造一份具有明确语义并且和已知密文相同的密文。
- Eve没有办法预测用户或系统将要选择的随机数。
- Eve不能根据公钥求出其对应的私钥。

Dolev-Yao模型具有重要意义，它被广泛地采纳为密码协议的标准威胁模型，现有的模型检测和定理证明技术大都基于Dolev-Yao模型。

1.4　关于本书的约定

为了方便读者更好地理解此书，也为了方便叙述，在本书中，我们对一些常

见的符号作统一说明：

Alice、Bob、Carlos：协议的参与方。他们可能相互认识，也可能不认识。一般来说，他们是诚实的主体。

Eve：一个不怀好意并且能力强大的攻击者。

S：代表服务器，也是协议的参与方。

KDC（Key Distribution Center）：密钥分发中心，是一个可信方。

TTP（Trusted Third Party）或者 Trent：可信第三方。

K_a：主体A的一个公开密钥或者A与S共享的一个对称密钥。

K_{ab}：主体A与主体B共享的一个密钥。

K_a^{-1}：对应于主体A公钥K_a的一个私钥。

$S_A(M)$：主体A对消息M签名的结果。

$\{M\}_k$：用密钥k对消息M加密。如果k是一个私钥的话，它表示一个签名。

$h()$：单向函数。

$h_k()$：带密钥的单向函数，密钥为k。

A → B：x：主体A向主体B发送消息x。

第二章 密码学基础

CHAPTER TWO
CRYPTOGRAPHY FOUNDATIONS

安全协议的基础是密码学。密码学是主要研究密码编码和密码分析的一门科学。密码编码和密码分析是一对矛与盾。直观地说，密码编码学是将一串有明确意义的字符变成一堆杂乱无章、毫无关系的字符；密码分析学主要研究在缺乏已知条件的情况下如何恢复这些杂乱无章的字符的本来面貌。任何一种密码编码方法都必须接受密码分析技术的检验。

密码学有着悠久的历史，它可以追溯到4000多年前。在这4000多年的历史中，密码学经历了重大的演变。早在几千年前的古埃及，人们就已经学会了使用最初级的密码；在公元前50年左右，凯撒大帝行军打仗时发明了最著名的古典密码——凯撒密码。在美国南北战争时期，军方使用了栅栏密码（Rail Fence Cipher）。第二次世界大战是密码学发展历史上的一个分水岭。在这之前，密码学几乎是军队、国防的专用技术，而在这之后，密码学得到了深入的研究、长足的发展和广泛的应用。这得益于1949年克劳德·香农（Claude Shannon）那篇现代密码学的开山著作《Communication Theory of Secrecy Systems》（Shannon，1949）。他将密码学建立在严密的数学理论上。然而，从1949年之后的接下来20年里，密码学的公开研究又少得可怜，主要是因为政府和相关机构（如美国国家安全局NSA）对该学科的保密。直到20世纪70年代初期，IBM的专家们发表了Feistel结构的密码学报告。

1976年，Diffie和Hellman发表了一篇文章《New Direction in Cryptography》。在这篇文章中，Diffie和Hellman第一次提出了公开密钥密码学[①]。公开密钥密码学看起来很奇怪，它用一个密钥去加密，却只能用另外一个密钥去解密。正是这样一篇文章，一石激起千层浪。从此之后，关于密码学的优秀研究成果源源不断地涌现出来。

① 另一种说法是：公开密钥密码学是由英国通信电子安全小组（CSEG）的James Ellis首先提出的，只不过CSEG没有公开相应的资料。这是历史的争论。

2.1 密码编码学

2.1.1 基本概念

消息（Message）被称为明文（Plain-text）。明文的取值范围称为明文空间。明文可以是二进制序列、文本、图片、声音或是一段录像。密码编码学主要研究如何隐藏明文的秘密而不被别人知晓。隐藏明文内容的过程称为加密，隐藏明文的方法称为加密算法，所使用的密钥称为加密密钥，加密后的消息被称为密文（Cipher-text），密文的取值范围称为密文空间。相应的，根据密文恢复消息内容的过程称为解密，恢复消息的方法称为解密算法，所使用的密钥称为解密密钥，密钥的取值范围称为密钥空间。加密算法和解密算法统称为密码算法。密码算法、明文空间、密文空间以及密钥空间，一同构成了密码系统。

加密和解密的关系及过程，如图2-1所示。

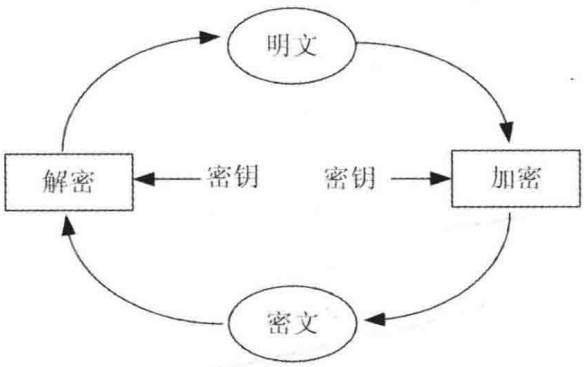

图2-1 加密和解密的关系及过程

输入明文M，在密钥K_1和加密算法E的作用下变为密文C。密文C在密钥K_2和解密算法D的作用下变为明文M，用数学公式可以表示为：

加密：

$$C = E(K_1, M) \tag{2-1}$$

解密：

$$M = D(K_2, C) \tag{2-2}$$

为了使加密后再解密可以恢复出明文，那么下述等式应当成立：

$$M = D(K_2, E(K_1, M)) \tag{2-3}$$

在式（2-1）~式（2-3）中，K_1和K_2不一定相等。

经过研究与实践，上述的加密算法E和解密算法D有很多种实现方式。根据不同的分类方法，可以将密码算法分为很多种类，例如：古典密码与现代密码、