信息安全专业系列教材

安全协议

Anquan
Xieyi

曹天杰　张永平　汪楚娇　编著

北京邮电大学出版社
www.buptpress.com

信息安全专业系列教材

安全协议

曹天杰　张永平　汪楚娇　编著

北京邮电大学出版社
·北京·

内容简介

本书全面和系统地讲述了安全协议的基本理论、安全协议的主要类型及安全协议的分析方法。围绕机密性、完整性、认证性、匿名性、公平性等实际需求，较全面地介绍满足各种应用需要的安全协议。

本书主要内容包括：安全协议概述、安全协议的密码学基础、基本的安全协议、认证与密钥建立协议、零知识证明、选择性泄露协议、数字签名变种、非否认协议、公平交换协议、安全电子商务协议、安全多方计算、安全协议的形式化分析。

本书内容全面、选材新颖、前后连贯，是江苏省高等学校精品教材建设立项项目。本书不仅可以作为信息安全专业本科生、研究生教材，也可以作为信息安全领域科研人员的参考书。

图书在版编目(CIP)数据

安全协议/曹天杰，张永平，汪楚娇编著. —北京：北京邮电大学出版社，2009

ISBN 978-7-5635-2049-7

Ⅰ. 安… Ⅱ. ①曹…②张…③汪… Ⅲ. 计算机网络—安全技术—通信协议 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2009)第 119609 号

书　　名：安全协议
作　　者：曹天杰　张永平　汪楚娇
责任编辑：崔　珞
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京忠信诚胶印厂
开　　本：787 mm×960 mm　1/16
印　　张：16
字　　数：356 千字
印　　数：1—3 000 册
版　　次：2009 年 8 月第 1 版　2009 年 8 月第 1 次印刷

ISBN 978-7-5635-2049-7　　定　价：26.00 元

前　言

密码学的用途是解决各种难题。当我们考虑现实世界中的应用时，常常遇到以下安全需求：机密性、完整性、认证性、匿名性、公平性等，密码学解决的各种难题围绕这些安全需求。安全协议是使用密码学完成某项特定的任务并满足安全需求的协议，又称密码协议，它在网络和分布式系统中有着大量的应用。

安全协议使用分组密码、公开密钥密码、散列函数、消息认证码、数字签名等密码原语构造，这些密码原语好比是砖头，安全协议就是利用砖头建筑的具有不同功能的大楼，比如写字楼、游泳馆、住宅等。我们知道即使砖头是结实的，如果设计得不好，大楼也是容易倒塌的，也是不安全的。本教材将讲解如何利用密码原语这些砖头构建一座座既要提供各种不同功能，又要安全牢固的“大楼”。

安全协议经过几十年的研究，已经取得了丰硕的成果，近些年的发展更是十分迅猛。遗憾的是，已有教材不能全面地反映安全协议的整个研究领域，不能让学生把握安全协议的全貌，达不到领会基本概念、掌握基础知识的目标。作为密码学的后续课程，国内 60 多所高校的信息安全专业大多设置了安全协议课程。因此，对安全协议进行系统的总结，出版一部安全协议的教材是十分必要的。

本书内容全面、选材新颖、前后连贯。讲述了安全协议的基本理论、安全协议的主要类型及安全协议的分析方法。

（1）内容全面。较全面地介绍了满足各种应用需要的安全协议，包括经典协议（即使有缺陷）、标准化的协议、现实中广泛应用的协议。

（2）选材新颖。作者一直从事安全协议方面的研究，能够把握这一领域发展的主流方向，因此在取材上能够把最新的研究成果引入教材。如认证密钥交换协议包括可否认的认证密钥交换协议、通信匿名的认证密钥交换协议、用户匿名的认证密钥交换协议，这些新概念进入教材能够开阔学生的视野，把学生引入到前沿课题中。教材编写中，有些例题、习题选自己出版的学术论文。

（3）前后连贯。教材要让人容易读懂，关键是条理清晰，概念清楚。在章节安排上，注意由浅入深、前后连贯。如承诺方案在后边的认证协议、签名协议中用到，签名协议在电子现金、电子拍卖协议中用到。因此，前后关系不能颠倒。讲解设计协议时，教材先介

绍现实中的安全需求，再介绍早期的协议，然后说明早期协议存在的缺陷，最后介绍改进后的协议，这样，能够让学生理解设计协议的整个思路。

本书共分为12章：第1章是安全协议概述。第2章介绍安全协议的密码学基础。从第3章到第12章，阐述安全协议中的一些基本理论和关键技术：基本的安全协议、认证与密钥建立协议、零知识证明、选择性泄露协议、数字签名变种、非否认协议、公平交换协议、安全电子商务协议、安全多方计算、安全协议的形式化分析。我们希望，通过学习这本教材，读者可以对安全协议有一个全面深入的了解。

本书已列入江苏省高等学校精品教材建设立项项目，并得到江苏省自然科学基金(No. BK2007035)、移动通信国家重点实验室开放研究基金(No. W200817)、中国矿业大学科技基金(No. 0D080309)的资助。在本书的写作过程中，研究生崔辉、杨珺涵、沈鹏、何涛参与了部分编写工作，在此特别致谢。

本书可以作为信息安全专业本科生、研究生教材，还可以供信息安全领域的科研人员参考。

由于作者水平有限，书中疏漏与错误之处在所难免，恳请广大同行和读者批评指正。编者联系方式为：tjcao@cumt.edu.cn，可随时联系索取课程资料。

作　者

目　　录

第 3 章 基本的安全协议

第 6 章 选择性泄露协议

第 7 章 数字签名变种

第 12 章　安全协议的形式化分析

第1章

安全协议概述

1.1 安全协议的概念

安全协议(Security Protocols),又称密码协议(Cryptographic Protocols),是以密码学为基础的消息交换协议,其目的是在网络环境中提供各种安全服务。

1.1.1 协议、算法与安全协议

在理解安全协议这一概念之前,首先要了解什么是协议。所谓协议,就是两个或两个以上的参与者采取一系列步骤以完成某项特定的任务。如 Internet 中的 IP 协议、TCP 协议、FTP 协议;现实生活中的购房协议、棋牌游戏规则等。这个定义有三层含义。

(1) 协议需要两个或两个以上的参与者。一个人可以通过执行一系列的步骤来完成一项任务,但它不构成协议。

(2) 在参与者之间呈现为消息处理和消息交换交替进行的一系列步骤。

(3) 通过执行协议必须能够完成某项任务或达成某项共识。

另外,协议还有其他特点。

(1) 协议中的每个参与者都必须了解协议,并且预先知道所要完成的所有步骤。

(2) 协议中的每个参与者都必须同意并遵循它。

(3) 协议必须是清楚的,每一步必须明确定义,并且不会引起误解。

(4) 协议必须是完整的,对每种情况必须规定具体的动作。

协议与算法不同。算法应用于协议中消息处理的环节,对不同的消息处理方式则要求不同的算法。

密码学的用途是解决各种难题。当考虑现实世界中的应用时,常常遇到以下安全需求:机密性、完整性、认证性、匿名性、公平性等,密码学解决的各种难题围绕这些安全需求。安全协议是使用密码学完成某项特定的任务并满足安全需求的协议,又称密码协议。在安全协议中,经常使用对称密码、公开密钥密码、单向函数、伪随机数生成器等密码算法,可以说,安全协议

就是在消息处理环节采用了若干密码算法的协议。具体而言，密码算法为传递的消息提供高强度的加、解密操作和其他辅助操作(如 Hash 运算)，而安全协议是在这些密码算法的基础上提供满足各种安全性要求的方案。安全协议中使用密码算法的目的是防止、发现窃听和欺骗。

安全协议的目的是在网络环境中为用户提供各种安全服务。安全协议运行在计算机网络或分布式系统中，为各方提供一系列步骤，借助于密码算法来实现密钥分配、身份认证以及安全地完成电子交易。

1.1.2 协议运行环境中的角色

1. 参与者

协议执行过程中的双方或多方，也就是人们常说的发送方和接收方。协议的参与者可能是完全信任的人，也可能是攻击者和完全不信任的人。比如认证协议中的发起者和响应者，零知识证明中的证明人和验证者，电子商务中的商家、银行和客户等。

2. 攻击者

攻击者(敌手)就是协议过程中企图破坏协议安全性和正确性的人。人们把不影响协议执行的攻击者称为被动攻击者，他们仅仅观察协议并试图获取信息。还有一类攻击者叫做主动攻击者，他们改变协议，在协议中引入新消息、修改消息或者删除消息等，达到欺骗、获取敏感信息、破坏协议等目的。

攻击者可能是协议的合法参与者，或是外部实体，或是两者的组合体，也可能是单个实体，或是合谋的多个实体。攻击者可能是协议参与者，他可能在协议期间撒谎，或者根本不遵守协议，这类攻击者叫做骗子，由于是系统的合法用户，因此也称为内部攻击者。攻击者也可能是外部的实体，他可能仅仅窃听以获取可用信息，也可能引入假冒的消息，这类攻击者称为外部攻击者。

3. 可信第三方

可信第三方(Trusted Third Party，TTP)是指在完成协议的过程中，值得信任的第三方，能帮助互不信任的双方完成协议。仲裁者是一类特殊的可信第三方，用于解决协议执行中出现的纠纷。仲裁者是在完成协议的过程中，值得信任的公正的第三方，“公正”意味着仲裁者在协议中没有既得利益，对参与协议的任何人也没有特别的利害关系。“值得信任”表示协议中的所有人都接受仲裁的结果，即仲裁者说的都是真实的，他做的仲裁是正确的，并且他将完成协议中涉及他的部分。其他可信第三方如密钥分发中心、认证中心等。

1.2 常用的安全协议

最常用、最基本的安全协议主要有以下四类。

1. 密钥建立协议

在网络通信中，通常使用对称密码算法用单独的密钥对每一次单独的会话加密，这个

密钥称为会话密钥。密钥建立协议的目的是在两个或者多个实体之间建立共享的会话密钥。可以采用对称密码体制或非对称密码体制建立会话密钥。有时借助于一个可信的服务器为用户分发密钥，这样的密钥建立协议称为密钥分发协议；也可以通过两个用户协商，共同建立会话密钥，这样的密钥建立协议称为密钥协商协议。

2. 认证协议

认证是对数据、实体标识的保证。数据起源认证意味着能够提供数据完整性，因为非授权地改变数据意味着数据来源的改变。实体认证是确认某个实体是它所声称的实体的过程，可能涉及证实用户的身份。认证协议主要防止假冒攻击。将认证和密钥建立协议结合在一起，是网络通信中最普遍应用的安全协议。

3. 电子商务协议

电子商务就是利用电子信息技术进行各种商务活动。电子商务协议中主体往往代表交易的双方，其利益目标不一致。因此，电子商务协议最关注公平性，即协议应保证交易双方都不能通过损害对方利益而得到其不应该得到的利益。常见的电子商务协议有电子现金协议、电子选举协议、拍卖协议、SET 协议等。

4. 安全多方计算协议

安全多方计算协议的目的是保证分布式环境中各参与方以安全的方式来共同执行分布式的计算任务。考虑到分布式计算的环境，在安全多方计算协议中，总假定协议在执行过程中会受到一个外部的实体，甚至是来自内部的一组参与方的攻击。这种假设很好地反映了网络环境下的安全需求。安全多方计算协议的两个最基本的安全要求是保证协议的正确性和各参与方私有输入的秘密性，即协议执行完后每个参与方都应该得到正确的输出，并且除此之外不能获知其他任何信息。安全多方计算协议包括抛币协议、广播协议、选举协议、电子投标和拍卖协议、电子现金协议、合同签署协议、匿名交易协议、保密信息检索、保密数据库访问、联合签名、联合解密等协议。

1.3 安全协议的安全性质

安全协议的目标就是保证某些安全性质在协议执行完毕时能够得以实现，换言之，评估一个安全协议是否是安全的就是检查其所要达到的安全性质是否受到攻击者的破坏，安全性质主要有认证性、机密性、完整性、非否认性和公平性等。利用密码算法提供的安全性质也称为安全服务。

1. 机密性

机密性是指确保信息不暴露给未授权的实体或进程，即信息不会被未授权的第三方所知。非授权读是对机密性的破坏。

机密性的目的是保护协议消息不被泄露给非授权拥有此消息的人，即使是攻击者观察到了消息的格式，他也无法从中得到消息的内容或提炼出有用的消息。保证协议消息

机密性的最直接的方法是对消息进行加密。加密使得消息由明文变为密文，并且任何人在不拥有密钥的情况下是不能解密消息的。

2. 完整性

完整性是指信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。非授权写是对完整性的破坏。

完整性的目的是保护协议消息不被非法改变、删除和替代。最常用的方法是封装和签名，即用签名或者 Hash 产生一个消息的摘要附在传送的消息上，作为验证消息完整性的依据，称为完整性校验值。一个关键性的问题是，通信双方必须事先达成有关算法的选择等款项的共识。

3. 认证性

认证可以对抗假冒攻击，用来确保身份，以便核查责任。在协议中，当某一成员（声称者）提交一个主体身份并声称他是那个主体时，需要运用认证以确认其身份是否如其声称所言，或者声称者需要拿出证明其真实身份的证据，这个过程称为认证的过程。在协议的实体认证中可以是单向的（认证一方），也可以是双向的（双方相互认证）。

4. 非否认性

非否认性包括收、发双方均不可否认（抵赖）已经发生的事实。一是源发证明，它提供给信息接收者以证据，这将使发送者谎称未发送过这些信息或者否认它的内容的企图不能得逞；二是交付证明，它提供给信息发送者以证据，这将使接收者谎称未接收过这些信息或者否认它的内容的企图不能得逞。

非否认性的目的是通过主体提供对方参与协议交换的证据以保证其合法利益不受侵害，即协议主体必须对自己的合法行为负责，而不能且无法事后否认。非否认协议的主体收集证据，以便事后能够向仲裁证明对方主体的确发送了或接收了消息。证据一般是以消息签名的形式出现的。

5. 公平性

公平性是电子支付协议的一个重要性质。其目的是保证参加协议的各方在协议执行的任何阶段都处于同等地位，当协议执行后，或者各方得到各自所需的，或者什么也得不到。

安全协议其他的安全性质还包括匿名与隐私属性、可验证性。在设计安全协议时，有时还要考虑计算高效性、通信高效性、强健性（鲁棒性）、易实现等。设计满足所有上述性质的协议是很困难的。

1.4 对安全协议的攻击

1983 年，Dolev 和 Yao（姚期智）发表了安全协议发展史上的一篇重要的论文。该论文的主要贡献有两点。第一点贡献是，将安全协议本身与安全协议采用的密码系统分开，在假定密码系统是“完善”的基础上讨论安全协议本身的正确性、安全性、冗余性等课题。